

Kaspersky

**Endpoint Security 10 Service Pack 2 for Windows**

# Cuprins

[Despre Kaspersky Endpoint Security 10 Service Pack 2 for Windows](#)[Noutăți](#)[Kitul de distribuire](#)[Organizarea protecției computerului](#)[Cerințe hardware și software](#)[Instalarea și eliminarea aplicației](#)[Instalarea aplicației](#)[Despre modalitățile de instalare a aplicației](#)[Instalarea aplicației folosind Expertul de instalare](#)[Pasul 1. Cum să te asiguri că îndeplinește computerul cerințele de instalare](#)[Pasul 2. Pagina de Bun venit pentru procedura de instalare](#)[Pasul 3. Vizualizarea Acordului de licență](#)[Pasul 4. Selectarea tipului de instalare](#)[Pasul 5. Selectarea componentelor aplicației de instalat](#)[Pasul 6. Selectarea directorului de destinație](#)[Pasul 7. Adăugarea de excluderi de la scanarea de viruși](#)[Pasul 8. Pregătirea instalării aplicației](#)[Pasul 9. Instalarea aplicației](#)[Instalarea aplicației din linia de comandă](#)[Instalarea la distanță a aplicației folosindu-se System Center Configuration Manager](#)[Descrierea setărilor fișierului setup.ini](#)[Expertul de configurare inițială](#)[Activarea aplicației](#)[Activarea cu un cod de activare](#)[Activarea utilizând un fișier cheie](#)[Selectarea funcțiilor de activat](#)[Finalizarea activării](#)[Analizarea sistemului de operare](#)[Finalizarea configurării inițiale a aplicației](#)[Declarația referitoare la Kaspersky Security Network](#)[Despre modalitățile de efectuare a unui upgrade pentru o versiune veche de aplicație](#)[Se elimină aplicația](#)[Despre modalitățile de eliminare a aplicației](#)

[Eliminarea aplicației folosind Expertul de instalare](#)[Pasul 1. Salvarea datelor aplicației pentru utilizare ulterioară](#)[Pasul 2. Confirmarea eliminării aplicației](#)[Pasul 3. Eliminarea aplicației. Finalizarea eliminării](#)[Eliminarea aplicației din linia de comandă](#)[Ștergerea obiectelor și a datelor rămase după operațiunea de testare a Agentului de Autentificare](#)[Interfața aplicației](#)[Pictograma aplicației din zona de notificare a barei de activități](#)[Meniul contextual al pictogramei aplicației](#)[Fereastra principală a aplicației](#)[Fila Configurare setări aplicație](#)[Fila Protecție și control aplicație](#)[Licența aplicației](#)[Despre Acordul de licență pentru utilizatorul final](#)[Despre licență](#)[Despre certificatul de licență](#)[Despre abonament](#)[Despre codul de activare](#)[Despre cheie](#)[Despre fișierul cheie](#)[Despre furnizarea datelor](#)[Vizualizarea informațiilor despre licență](#)[Achiziționarea unei licențe](#)[Reînnoirea unei licențe](#)[Reînnoirea abonamentului](#)[Vizitarea site-ului Web al furnizorului de servicii](#)[Despre metoda de activare a aplicației](#)[Utilizarea Expertului de activare pentru activarea aplicației](#)[Activarea aplicației din linia de comandă](#)[Pornirea și oprirea aplicației](#)[Activarea și dezactivarea pornirii automate a aplicației](#)[Pornirea și oprirea manuală a aplicației](#)[Trecerea în pauză și reluarea protecției și controlului computerului](#)[Protejarea sistemului de fișiere al computerului. Antivirus pentru fișiere](#)[Despre Antivirusul pentru fișiere](#)[Activarea și dezactivarea Antivirusului pentru fișiere](#)[Trecerea automată în pauză a Antivirusului pentru fișiere](#)[Configurarea Antivirusului pentru fișiere](#)

[Schimbarea nivelului de securitate](#)

[Schimbarea acțiunii efectuate de Antivirusul pentru fișiere asupra fișierelor infectate](#)

[Editarea domeniului de protecție al Antivirusului pentru fișiere](#)

[Utilizarea analizorului euristic cu Antivirusul pentru fișiere](#)

[Utilizarea tehnologiilor de scanare la funcționarea Antivirusului pentru fișiere](#)

[Optimizarea scanării de fișiere](#)

[Scanarea fișierelor compuse](#)

[Schimbarea modului de scanare](#)

[Protecția pentru e-mail. Antivirus pentru e-mail](#)

[Despre Antivirusul pentru e-mail](#)

[Activarea și dezactivarea Antivirusului pentru e-mail](#)

[Configurarea Antivirusului pentru e-mail](#)

[Schimbarea nivelului de securitate a e-mailului](#)

[Schimbarea acțiunii de efectuat asupra mesajelor de e-mail infectate](#)

[Editarea domeniului de protecție al Antivirusului pentru e-mail](#)

[Scanarea fișierelor compuse atașate la mesaje de e-mail](#)

[Filtrarea atașărilor la mesaje de e-mail](#)

[Scanarea e-mailurilor în Microsoft Office Outlook](#)

[Configurarea scanării e-mailului în Outlook](#)

[Configurarea scanării mesajelor de e-mail folosind Kaspersky Security Center](#)

[Protecția computerului pe Internet. Antivirus pentru Web](#)

[Despre Antivirusul pentru Web](#)

[Activarea și dezactivarea Antivirusului pentru Web](#)

[Configurarea Antivirusului pentru Web](#)

[Schimbarea nivelului de securitate a traficului Web](#)

[Schimbarea acțiunii de efectuat asupra obiectelor de trafic Web rău intenționate](#)

[Scanarea cu Antivirusul pentru Web a adreselor URL în bazele de date cu adrese Web periculoase și de phishing](#)

[Utilizarea analizorului euristic cu Antivirusul pentru Web](#)

[Editarea listei de adrese URL de încredere](#)

[Protecția traficului prin clientul MI. Antivirus IM](#)

[Despre componenta Antivirus MI](#)

[Activarea și dezactivarea componentei Antivirus MI](#)

[Configurarea componentei Antivirus MI](#)

[Crearea domeniului de protecție al componentei Antivirus MI](#)

[Scanarea adreselor URL în raport cu bazele de date periculoase și de phishing utilizând componenta Antivirus MI](#)

[Monitorizare sistem](#)

[Despre componenta Monitorizare sistem](#)

[Activare și dezactivare Monitorizare sistem](#)

[Configurarea componentei Monitorizare sistem](#)

[Activarea sau dezactivarea protecției împotriva exploitelor](#)

[Alegerea acțiunii de efectuat la detectarea unei activități rău intenționate într-un program](#)

[Activarea și dezactivarea restaurării acțiunilor programelor periculoase în timpul dezinfectării](#)

## [Firewall](#)

[Despre Firewall](#)

[Activarea sau dezactivarea Firewall](#)

[Despre regulile de rețea](#)

[Despre starea conexiunii de rețea](#)

[Modificarea stării conexiunii de rețea](#)

[Gestionarea regulilor pentru pachetele de rețea](#)

[Crearea și editarea unei reguli pentru pachete de rețea](#)

[Activarea sau dezactivarea unei reguli pentru pachete de rețea](#)

[Modificarea acțiunii Firewall pentru o regulă pentru pachete de rețea](#)

[Modificarea priorității unei reguli pentru pachete de rețea](#)

[Administrarea regulilor de rețea ale aplicației](#)

[Crearea și editarea unei reguli de rețea pentru o aplicație](#)

[Activarea și dezactivarea unei reguli de rețea pentru o aplicație](#)

[Modificarea acțiunii Firewall pentru o regulă de rețea pentru o aplicație](#)

[Modificarea priorității unei reguli de rețea pentru o aplicație](#)

[Monitor rețea](#)

[Despre Monitor rețea](#)

[Pornirea instrumentului Monitor rețea](#)

## [Blocare atacuri de rețea](#)

[Despre componenta Blocare atacuri de rețea](#)

[Activarea și dezactivarea Blocare atacuri de rețea](#)

[Setările componentei Blocare atacuri de rețea](#)

[Editarea setărilor folosite la blocarea unui computer atacator](#)

[Configurarea adreselor de excluderi de la blocare](#)

## [Prevenire atac BadUSB](#)

[Despre Prevenire atac BadUSB](#)

[Instalarea componentei Prevenire atac BadUSB](#)

[Activarea și dezactivarea componentei Prevenire atac BadUSB](#)

[Permiterea sau interzicerea utilizării tastaturii virtuale pentru autorizare](#)

[Autorizarea tastaturii](#)

## [Componenta Control pornire aplicații](#)

[Despre componenta Control pornire aplicații](#)

[Activarea și dezactivarea componentei Control pornire aplicații](#)

[Limitările funcționalității Control pornire aplicații](#)

[Despre regulile componentei Control pornire aplicații](#)

[Gestionarea regulilor componentei Control pornire aplicații](#)

[Adăugarea și editarea unei reguli a componentei Control pornire aplicații](#)

[Adăugarea unei condiții de declanșare pentru o regulă a componentei Control pornire aplicații](#)

[Modificarea stării unei reguli a componentei Control pornire aplicații](#)

[Testarea regulilor componentei Control la pornirea aplicației](#)

[Editarea șabloanelor de mesaje aferente componentei Control pornire aplicații](#)

[Despre modurile de funcționare a componentei Control pornire aplicații](#)

[Selectarea modului pentru Control pornire aplicații](#)

[Administrarea regulilor pentru Control la pornirea aplicației folosind Kaspersky Security Center](#)

[Colectarea informațiilor despre aplicațiile instalate pe computerele utilizatorilor](#)

[Crearea categoriilor de aplicații](#)

[Crearea regulilor pentru Control la pornirea aplicației folosind Kaspersky Security Center](#)

[Modificarea stării unei reguli a componentei Control pornire aplicații folosind Kaspersky Security Center](#)

[Componenta Control privilegii aplicații](#)

[Despre Control privilegii aplicații](#)

[Limitările controlului pentru dispozitive audio și video](#)

[Activarea și dezactivarea componentei Control privilegii aplicații](#)

[Administrarea grupurilor de încredere pentru aplicații](#)

[Configurarea setărilor pentru alocarea aplicațiilor în grupuri de încredere](#)

[Modificarea unui grup de încredere](#)

[Selectarea unui grup de încredere pentru aplicații lansate înainte de Kaspersky Endpoint Security](#)

[Gestionarea regulilor de Control aplicații](#)

[Modificarea regulilor de control al aplicațiilor pentru grupurile de încredere și pentru grupurile de aplicații](#)

[Editarea unei reguli de control al aplicației](#)

[Dezactivarea descărcărilor și a actualizărilor pentru regulile de control al aplicațiilor din baza de date Kaspersky Security Network](#)

[Dezactivarea moștenirii de restricții din procesul părinte](#)

[Excluderea acțiunilor anumitor aplicații de la regulile de control pentru aplicații](#)

[Eliminarea regulilor de control al aplicațiilor învechite](#)

[Protejarea resurselor sistemului de operare și a datelor de identitate](#)

[Adăugarea unei categorii de resurse protejate](#)

[Adăugarea unei resurse protejate](#)

[Dezactivarea protecției resursei](#)

[Monitor de vulnerabilități](#)

[Despre Monitorul de vulnerabilități](#)

## [Activarea și dezactivarea Monitorului de vulnerabilități](#)

### [Componenta Control dispozitive](#)

#### [Despre componenta Control dispozitive](#)

#### [Activarea și dezactivarea componentei Control dispozitive](#)

#### [Despre regulile de acces la dispozitive și la magistrale de conectare](#)

#### [Despre dispozitivele de încredere](#)

#### [Decizii standard privind accesul la dispozitive](#)

#### [Editarea unei reguli de acces la dispozitive](#)

#### [Adăugarea rapoartelor la sau excluderea rapoartelor din jurnalul de evenimente](#)

#### [Adăugarea unei rețele Wi-Fi la lista de încredere](#)

#### [Editarea unei reguli de acces la magistrale de conectare](#)

#### [Acțiuni cu dispozitive de încredere](#)

##### [Adăugarea unui dispozitiv la lista De încredere din interfața aplicației](#)

##### [Adăugarea dispozitivelor la lista De încredere pe baza modelului sau ID-ului dispozitivului](#)

##### [Adăugarea dispozitivelor la lista De încredere pe baza măștii de ID-uri dispozitiv](#)

##### [Configurarea accesului utilizatorului la un dispozitiv de încredere](#)

##### [Eliminarea unui dispozitiv din lista de dispozitive de încredere](#)

#### [Editarea șabloanelor de mesaje ale componentei Control dispozitive](#)

#### [Obținerea accesului la un dispozitiv blocat](#)

#### [Crearea unei chei pentru accesarea unui dispozitiv blocat folosind Kaspersky Security Center](#)

### [Componenta Control Web](#)

#### [Despre componenta Control Web](#)

#### [Activarea și dezactivarea componentei Control Web](#)

#### [Categorii de conținut pentru resurse Web](#)

#### [Despre regulile de acces la resurse Web](#)

#### [Acțiuni asupra regulilor de acces la resurse Web](#)

##### [Adăugarea și editarea unei reguli de acces la resurse Web](#)

##### [Atribuirea de priorități regulilor de acces la resurse Web](#)

##### [Testarea regulilor de acces la resurse Web](#)

##### [Activarea și dezactivarea unei reguli de acces la resurse Web](#)

#### [Migrarea regulilor de acces la resurse Web de la versiuni anterioare ale aplicației](#)

#### [Exportul și importul unei liste de adrese de resurse Web](#)

#### [Editarea măștilor pentru adrese de resurse Web](#)

#### [Editarea șabloanelor de mesaje ale componentei Control Web](#)

### [Senzor Kata Endpoint](#)

#### [Despre Senzorul Kata Endpoint](#)

#### [Activarea sau dezactivarea componentei Senzor KATA Endpoint](#)

### [Criptare date](#)

[Activarea afișării setărilor de criptare în politica aplicației Kaspersky Security Center](#)

[Despre criptarea datelor](#)

[Limitările funcționalității de criptare](#)

[Modificarea algoritmului de criptare](#)

[Activarea tehnologiei Single Sign-On \(SSO\)](#)

[Considerații speciale pentru criptarea fișierelor](#)

[Criptarea fișierelor de pe unitățile locale ale computerului](#)

[Criptarea fișierelor de pe unitățile locale ale computerului](#)

[Crearea regulilor de acces la fișiere criptate pentru aplicații](#)

[Criptarea fișierelor create sau modificate de aplicații specifice](#)

[Generarea unei reguli de decriptare](#)

[Decriptarea fișierelor de pe unitățile locale ale computerului](#)

[Crearea pachetelor criptate](#)

[Extragerea pachetelor criptate](#)

[Criptarea unităților amovibile](#)

[Lansarea criptării unităților amovibile](#)

[Adăugarea unei reguli de criptare pentru unități amovibile](#)

[Editarea unei reguli de criptare pentru unități amovibile](#)

[Activarea modului portabil pentru accesarea fișierelor criptate de pe unități amovibile](#)

[Decriptarea unităților amovibile](#)

[Criptarea unităților de hard disk](#)

[Despre criptarea unităților de hard disk](#)

[Criptarea unităților de hard disk folosind tehnologia Kaspersky Disk Encryption](#)

[Criptarea unităților de hard disk folosind tehnologia Criptare unitate BitLocker](#)

[Crearea unei liste de unități de hard disk excluse de la criptare](#)

[Decriptarea unităților de hard disk](#)

[Gestionarea Agentului de Autentificare](#)

[Folosirea unui simbol/card inteligent cu Agentul de Autentificare](#)

[Editarea mesajelor de ajutor ale Agentului de Autentificare](#)

[Suport limitat pentru caractere în mesajele de ajutor pentru Agentul de Autentificare](#)

[Selectarea nivelului de urmărire pentru Agentul de Autentificare](#)

[Gestionarea conturilor Agentului de Autentificare](#)

[Adăugarea unei comenzi pentru crearea unui cont de Agent de Autentificare](#)

[Adăugarea comenzii de editare pentru un cont de Agent de Autentificare](#)

[Adăugarea unei comenzi pentru ștergerea unui cont de Agent de Autentificare](#)

[Restaurarea acreditărilor pentru contul de Agent de Autentificare](#)

[Răspunsul la solicitarea unui utilizator de restaurare a acreditărilor pentru contul de Agent de Autentificare](#)

## Vizualizarea detaliilor de criptare date

Despre starea de criptare

Vizualizarea stării de criptare

Vizualizarea statisticilor de criptare în panourile de detalii ale Kaspersky Security Center

Vizualizarea erorilor de criptare fișiere pe unitățile locale ale computerului

Vizualizarea raportului de criptare a datelor

## Administrarea fișierelor criptate cu funcționalitate de criptare fișiere limitată

Accesarea fișierelor criptate fără o conexiune la Kaspersky Security Center

Acordarea dreptului unui utilizator de a accesa fișiere criptate fără a conexiune la Kaspersky Security Center

Editarea șabloanelor de mesaje pentru acces la fișiere criptate

## Lucrul cu dispozitive criptate atunci când nu există acces la acestea

Obținerea accesului la dispozitive criptate prin intermediul interfeței aplicației

Acordarea accesului utilizatorului la dispozitive criptate

Furnizarea unei chei de recuperare pentru unități de hard disk criptate cu BitLocker

Crearea fișierului executabil fdert.exe al utilitarului Restaurare

Restaurarea datelor pe dispozitivele criptate folosind Utilitarul de restaurare

Răspunsul la solicitarea unui utilizator de a restaura date pe dispozitive criptate

## Restaurarea accesului la date criptate după o eroare de sistem

## Crearea unui disc de recuperare pentru sistemul de operare

## Protecție rețea

Despre Protecție rețea

Configurarea setărilor pentru monitorizarea traficului de rețea

Activarea monitorizării tuturor porturilor de rețea

Crearea unei liste de porturi de rețea monitorizate

Crearea unei liste de aplicații pentru care sunt monitorizate toate porturile de rețea

## Actualizarea bazelor de date și modulelor aplicației

Despre actualizarea bazelor de date și modulelor aplicației

Despre sursele de actualizare

Configurarea setărilor pentru actualizare

Adăugarea unei surse de actualizare

Selectarea regiunii pentru serverul de actualizare

Configurarea actualizărilor dintr-un director partajat

Selectarea modului de executare a activității de actualizare

Pornirea unei activități de actualizare utilizând drepturile altui cont de utilizator

Configurarea actualizărilor pentru modulele aplicației

Pornirea și oprirea unei activități de actualizare

Derularea înapoi a celei mai recente actualizări



[Configurarea setărilor pentru serverul proxy](#)[Scanarea computerului](#)[Despre activitățile de scanare](#)[Pornirea și oprirea unei activități de scanare](#)[Configurarea setărilor pentru o activitate de scanare](#)[Schimbarea nivelului de securitate](#)[Schimbarea acțiunii de efectuat asupra fișierelor infectate](#)[Generarea unei liste de obiecte de scanat](#)[Selectarea unui tip de fișiere de scanat](#)[Optimizarea scanării de fișiere](#)[Scanarea fișierelor compuse](#)[Utilizarea metodelor de scanare](#)[Utilizarea tehnologiilor de scanare](#)[Selectarea modului de executare pentru activitatea de scanare](#)[Pornirea unei activități de scanare din contul altui utilizator](#)[Scanarea unităților amovibile atunci când sunt conectate la computer](#)[Tratarea fișierelor neprocesate](#)[Despre fișierele neprocesate](#)[Gestionarea listei de fișiere neprocesate](#)[Pornirea unei activități de scanare particularizată pentru fișiere neprocesate](#)[Ștergerea fișierelor din lista de fișiere neprocesate](#)[Scanarea de vulnerabilități](#)[Vizualizarea informațiilor despre vulnerabilitățile aplicațiilor în curs de executare](#)[Despre activitatea Scanare de vulnerabilități](#)[Pornirea și oprirea activității Scanare de vulnerabilități](#)[Configurarea setărilor Scanare de vulnerabilități](#)[Crearea unui domeniu de scanare de vulnerabilități](#)[Selectarea modului de executare pentru activitatea Scanare de vulnerabilități](#)[Pornirea activității Scanare de vulnerabilități utilizând drepturile unui alt cont de utilizator](#)[Gestionarea listei de vulnerabilități](#)[Despre lista de vulnerabilități](#)[Repornirea unei activități Scanare de vulnerabilități](#)[Remediarea unei vulnerabilități](#)[Ascunderea înregistrărilor din lista de vulnerabilități](#)[Filtrarea listei de vulnerabilități după nivelul de gravitate](#)[Filtrarea listei de vulnerabilități după valorile de stare Remediat și Ascuns](#)[Verificarea integrității modulelor aplicației](#)[Despre activitatea Verificare integritate](#)

[Pornirea și oprirea unei activități Verificare integritate](#)

[Selectarea modului de executare pentru activitatea de verificare a integrității](#)

## [Gestionarea rapoartelor](#)

[Principiile gestionării rapoartelor](#)

[Configurarea setărilor pentru rapoarte](#)

[Configurarea duratei maxime de stocare a rapoartelor](#)

[Configurarea dimensiunii maxime a fișierului raport](#)

[Vizualizarea rapoartelor](#)

[Vizualizarea informațiilor despre eveniment în raport](#)

[Salvarea unui raport într-un fișier](#)

[Golirea rapoartelor](#)

## [Serviciul de notificare](#)

[Despre notificările aplicației Kaspersky Endpoint Security](#)

[Configurarea serviciului de notificare](#)

[Configurarea setărilor pentru jurnalul de evenimente](#)

[Configurarea afișării și livrării notificărilor](#)

[Configurarea afișării avertizărilor despre starea aplicației în zona de notificare](#)

## [Gestionarea carantinei și a copiilor de rezervă](#)

[Despre carantină și copiile de rezervă](#)

[Configurarea setărilor pentru Carantină și Copie de rezervă](#)

[Configurarea duratei maxime de stocare a fișierelor în Carantină și de stocare a copiilor de fișiere în Copie de rezervă](#)

[Configurarea dimensiunii maxime a zonelor Carantină și Copie de rezervă](#)

## [Gestionarea zonei Carantină](#)

[Activarea și dezactivarea scanării fișierelor din carantină în urma unei actualizări](#)

[Pornirea unei activități de scanare particularizată pentru fișierele din carantină](#)

[Restaurarea fișierelor din carantină](#)

[Ștergerea fișierelor din carantină](#)

## [Gestionarea copiilor de rezervă](#)

[Restaurarea fișierelor din Copie de rezervă](#)

[Ștergerea copiilor de rezervă ale fișierelor din Copie de rezervă](#)

## [Setările avansate ale aplicației](#)

[Crearea și folosirea unui fișier de configurare](#)

### [Zona de încredere](#)

[Despre zona de încredere](#)

[Crearea unei excluderi de la scanare](#)

[Modificarea unei excluderi de la scanare](#)

[Ștergerea unei excluderi de la scanare](#)

[Activarea și dezactivarea unei excluderi de la scanare](#)

[Editarea listei de aplicații de încredere](#)

[Activarea și dezactivarea regulilor pentru zona de încredere pentru o aplicație din lista de aplicații de încredere](#)

[Folosirea depozitului de certificate de sistem de încredere](#)

[Autoprotecția aplicației Kaspersky Endpoint Security](#)

[Despre Autoprotecția aplicației Kaspersky Endpoint Security](#)

[Activarea sau dezactivarea Autoprotecției](#)

[Activarea sau dezactivarea protecției împotriva controlului la distanță](#)

[Acceptarea aplicațiilor de administrare la distanță](#)

[Performanțele aplicației Kaspersky Endpoint Security și compatibilitatea acesteia cu alte aplicații](#)

[Despre performanțele aplicației Kaspersky Endpoint Security și compatibilitatea acesteia cu alte aplicații](#)

[Selectarea tipurilor de obiecte detectabile](#)

[Activarea sau dezactivarea tehnologiei de dezinfectare avansată pentru stații de lucru](#)

[Activarea sau dezactivarea tehnologiei de dezinfectare avansată pentru servere de fișiere](#)

[Activarea sau dezactivarea modului de economisire a energiei](#)

[Activarea sau dezactivarea cedării de resurse pentru alte aplicații](#)

[Protecția prin parolă](#)

[Despre restricționarea accesului la Kaspersky Endpoint Security](#)

[Activarea și dezactivarea protecției prin parolă](#)

[Modificarea parolei de acces la Kaspersky Endpoint Security](#)

[Despre folosirea unei parole temporare](#)

[Crearea unei parole temporare folosind Consola de administrare Kaspersky Security Center](#)

[Aplicarea unei parole temporare în interfața Kaspersky Endpoint Security](#)

[Administrarea la distanță a aplicației prin Kaspersky Security Center](#)

[Despre gestionarea aplicației prin Kaspersky Security Center](#)

[Considerații speciale pentru lucru cu versiuni diferite ale plug-inurilor de administrare](#)

[Pornirea și oprirea Kaspersky Endpoint Security pe un computer client](#)

[Configurarea setărilor Kaspersky Endpoint Security](#)

[Gestionarea activităților](#)

[Despre activitățile pentru Kaspersky Endpoint Security](#)

[Configurarea modului de gestionare a activităților](#)

[Crearea unei activități locale](#)

[Crearea unei activități de grup](#)

[Crearea unei activități pentru o selecție de dispozitive](#)

[Pornirea, oprirea, suspendarea și reluarea unei activități](#)

[Editarea setărilor unei activități](#)

[Gestionarea politicilor](#)

[Despre politici](#)

[Crearea unei politici](#)

[Editarea setărilor de politică](#)

[Selectarea setărilor care vor fi afișate în politica aplicației Kaspersky Security Center](#)

[Trimiterea de mesaje ale utilizatorului către serverul Kaspersky Security Center](#)

[Vizualizarea mesajelor utilizatorului în spațiul de stocare a evenimentelor din Kaspersky Security Center](#)

[Participarea la Kaspersky Security Network](#)

[Despre participarea la Kaspersky Security Network](#)

[Activarea și dezactivarea utilizării serviciului Kaspersky Security Network](#)

[Verificarea conexiunii la serviciul Kaspersky Security Network](#)

[Verificarea reputației unui fișier în Kaspersky Security Network](#)

[Protecție îmbunătățită cu Kaspersky Security Network](#)

[Surse de informații despre aplicație](#)

[Contactarea Serviciului de asistență tehnică](#)

[Cum se obține asistență tehnică](#)

[Asistența tehnică prin telefon](#)

[Asistența tehnică prin Kaspersky CompanyAccount](#)

[Colectarea de informații pentru serviciul de asistență tehnică](#)

[Crearea unui fișier de urmărire](#)

[Conținutul și zona de stocare pentru fișierele de urmărire](#)

[Activarea sau dezactivarea transmiterii către Kaspersky a fișierelor imagine memorie și a fișierelor de urmărire](#)

[Trimiterea de fișiere către serverul serviciului de Asistență tehnică](#)

[Activarea și dezactivarea protecției pentru fișierele imagine și de urmărire](#)

[Glosar](#)

[Activitate](#)

[Actualizare](#)

[Adresă normalizată pentru o resursă Web](#)

[Agent de autentificare](#)

[Agent de rețea](#)

[Alarmă falsă](#)

[Amprentă certificat](#)

[Analiză euristică](#)

[Analiză semnături](#)

[Arhivă](#)

[Bază de date de adrese Web de phishing](#)

[Bază de date de adrese Web periculoase](#)

[Baze de date antivirus](#)

[Carantină](#)[Certificat](#)[Certificat licență](#)[Cheie activă](#)[Cheie suplimentară](#)[Conector agent de rețea](#)[Copie de rezervă](#)[Corecție](#)[Dezinfectare](#)[Domeniu de protecție](#)[Domeniu de scanare](#)[Emitent certificat](#)[Exploit](#)[Fișier infectabil](#)[Fișier infectat](#)[Fișier probabil infectat](#)[Grup de administrare](#)[Listă neagră de adrese](#)[Manager de fișiere portabil](#)[Mască de fișier](#)[Modulele aplicației](#)[Mutarea fișierelor în Carantină](#)[Obiect OLE](#)[Phishing](#)[Server de administrare](#)[Serviciu de rețea](#)[Setări pentru activitate](#)[Setări pentru aplicație](#)[Subiect certificat](#)[Trusted Platform Module](#)[Informații despre codurile de la terți](#)[Note privind mărcile comerciale](#)

## Despre Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Această secțiune descrie funcțiile, componentele și kitul de distribuire pentru Kaspersky Endpoint Security și furnizează o listă de cerințe hardware și software pentru Kaspersky Endpoint Security.

# Noutăți

Kaspersky Endpoint Security 10 Service Pack 2 for Windows oferă următoarele caracteristici și îmbunătățiri:

## 1. Componenta Control pornire aplicații:

- Sisteme de operare pentru server acceptate.
- Controlează descărcările modulelor DLL și driverelor.
- Gestionează lista de obiecte din activitatea de inventar (module DLL și fișiere script).
- Controlează obiecte pe baza unui criteriu nou – după atributele certificatului de semnătură digitală.
- Generează un raport privind pornirile de test ale aplicațiilor blocate.
- Acceptă două moduri de operare pentru Control pornire aplicații: Listă neagră și Listă albă.
- Utilizează codul hash SHA256 pentru controlul și inventarul obiectelor.
- Controlează executarea scripturilor de la interpretorul PowerShell.
- Folosește depozitul de certificate de sistem de încredere.

## 2. Administrarea Microsoft BitLocker permite criptarea unităților de hard disk cu ajutorul tehnologiei BitLocker de la Microsoft:

- Administrare la distanță a criptării.
- Monitorizare a dispozitivelor criptate.
- Crearea de rapoarte despre criptarea dispozitivelor.
- Restaurare a accesului la dispozitive criptate.

## 3. Kaspersky Disk Encryption:

- Suport pentru introducerea acreditărilor în mediul preboot al Agentului de Autentificare folosind o tastatură virtuală.
- Suport pentru modul Criptare pentru criptarea numai a spațiului ocupat de pe un dispozitiv.
- Suport pentru criptare pe tablete (MS Surface versiunile 3 și 4).

#### 4. Componenta Control drepturi aplicații:

- Controlează accesul aplicațiilor la dispozitive de înregistrare audio și video.

#### 5. Componenta Control Web:

- Configurează regulile de acces la resurse Web pentru categorii suplimentare de resurse Web.

#### 6. Componenta Control dispozitive:

- Înregistrează în jurnal evenimente asociate cu ștergerea și salvarea fișierelor pe dispozitive USB.
- Generează o listă de rețele Wi-Fi de încredere pe baza următoarelor setări: nume, tip de criptare și tip de autentificare.
- Gestionare drepturile de acces ale utilizatorului pentru operațiunile de citire și scriere fișiere pe discuri CD/DVD.

#### 7. Antivirus pentru e-mail:

- Este capabil să șteargă și să redenumescă anumite tipuri de fișiere din arhive pentru scanarea de către componenta Antivirus pentru e-mail.

#### 8. Kaspersky Security Network:

- Afișează KSN ca motiv pentru o decizie privind metoda de procesare a obiectelor în rapoarte Kaspersky Endpoint Security și rapoarte Kaspersky Security Center.
- Trimite la KSN o interogare privind reputația unui fișier selectat.
- Afișează starea de disponibilitate a serverelor KSN pentru computere client pe care este instalat Kaspersky Endpoint Security.

## Kitul de distribuire

Kitul de distribuire Kaspersky Endpoint Security conține următoarele fișiere:

- Fișierele necesare pentru [instalarea aplicației](#) folosind oricare dintre metodele disponibile:
- Fișierele pachetului de actualizare folosite în cursul instalării aplicației.
- Fișierul klcfginst.msi pentru instalarea plug-inului de administrare Kaspersky Endpoint Security prin intermediul Kaspersky Security Center.

- Fișierul ksn\_<ID limbă>.txt, în care poți vedea termenii pentru [participarea la Kaspersky Security Network](#).
- Fișierul license.txt, în care poți vedea [Acordul de licență pentru utilizatorul final](#).
- Fișierul incompatible.txt, care conține o listă de programe software incompatibile.
- Fișierul installer.ini, care conține setările interne ale kitului de distribuire.

Nu se recomandă modificarea acestor setări. Dacă dorești să modifice opțiunile de instalare, folosește [fișierul setup.ini](#).

Trebuie să dezarhivezi kitul de distribuire pentru a accesa fișierele.

## Organizarea protecției computerului

Kaspersky Endpoint Security asigură o protecție complexă a computerului împotriva diferitelor tipuri de amenințări, împotriva atacurilor de rețea și a celor de tip phishing.

Fiecare tip de amenințare este tratat de o componentă specială. Componentele pot fi activate sau dezactivate în mod individual, iar setările acestora pot fi configurate.

În afară de protecția în timp real pe care o oferă componentele aplicației, îți recomandăm să *scanezi* computerul în vederea detectării virușilor și a altor amenințări. Acest lucru contribuie la eliminarea posibilității de răspândire a programelor malware nedetectate de componentele protecției din cauza unei setări reduse a nivelului de securitate sau din alte motive.

Pentru a te asigura că aplicația Kaspersky Endpoint Security este actualizată, trebuie să *actualizezi* bazele de date și modulele pe care le utilizează aplicația. Aplicația se actualizează automat în mod implicit, dar, dacă este necesar, poți actualiza manual bazele de date și modulele aplicației.

Următoarele componente ale aplicației reprezintă componente de control:

- **Control pornire aplicații.** Această componentă monitorizează încercările utilizatorilor de a porni aplicații și reglementează pornirea aplicațiilor.
- **Control drepturi aplicații.** Această componentă înregistrează acțiunile aplicațiilor în sistemul de operare și reglementează activitatea aplicațiilor în funcție de grupul de încredere din care face parte o anumită aplicație. Pentru fiecare grup de aplicații este specificat un set de reguli. Aceste reguli reglementează accesul aplicațiilor la datele utilizatorului și la resursele sistemului de operare. Aceste date includ fișiere de ale utilizatorului (directorul My Documents (Documentele mele), module cookie, informații despre activitatea utilizatorului) și fișiere, directoare și chei de registru care conțin setări și informații importante din aplicațiile utilizate cel mai frecvent.



- **Monitor de vulnerabilități.** Componenta Monitor de vulnerabilități execută o scanare în timp real pentru a detecta vulnerabilități în aplicațiile care sunt pornite sau de execută pe computerul utilizatorului.
- **Control dispozitive.** Această componentă îți permite să setezi restricții flexibile asupra accesului la dispozitive de stocare a datelor (precum unități de hard disk, unități amovibile, unități cu bandă și discuri CD/DVD), echipamente pentru transmitere de date (precum modemuri), echipamente care transferă date pe suporturi fizice (precum imprimante) sau interfețe pentru conectarea de dispozitive la computere (precum USB, Bluetooth și infraroșu).
- **Control Web.** Această componentă îți permite să setezi restricții flexibile asupra accesului la resurse Web pentru diverse grupuri de utilizatori.

Funcționarea componentelor de control se bazează pe următoarele reguli:

- Componenta Control pornire aplicații folosește [reguli de Control la pornirea aplicației](#).
- Componenta Control drepturi aplicații folosește [reguli de Control aplicații](#).
- Componenta Control dispozitive folosește [reguli de acces la dispozitive și reguli de acces la magistrala de conectare](#).
- Componenta Control Web folosește [reguli de acces la resurse Web](#).

Următoarele componente ale aplicației reprezintă componente de protecție:

- **Antivirus pentru fișiere.** Această componentă protejează sistemul de fișiere al computerului împotriva infectării. Componenta Antivirus pentru fișiere pornește împreună cu Kaspersky Endpoint Security, rămâne permanent activă în memoria computerului și scanează toate fișierele deschise, salvate sau lansate pe computer și pe unitățile conectate. Componenta Antivirus pentru fișiere interceptează orice încercare de accesare a unui fișier și scanează fișierul de viruși și alte amenințări.
- **Monitorizare sistem.** Această componentă ține evidența activității aplicației pe computer și oferă aceste informații celorlalte componente pentru a asigura o protecție mai eficientă a computerului.
- **Antivirus pentru e-mail.** Această componentă scanează mesaje de e-mail primite și trimise în vederea detectării de viruși și alte amenințări.
- **Antivirus pentru Web.** Această componentă scanează traficul care ajunge pe computerul utilizatorului prin protocoalele HTTP și FTP și verifică dacă adresele URL se numără printre adresele Web listate ca fiind rău intenționate sau de phishing.
- **Antivirus MI.** Această componentă scanează traficul care ajunge pe computer prin protocoalele clienților de MI. Componenta îți permite utilizarea în siguranță a multor clienți de MI.

- **Firewall.** Această componentă protejează datele stocate pe computer și blochează majoritatea amenințărilor posibile pentru sistemul de operare, atunci când computerul este conectat la Internet sau la o rețea locală. Componenta filtrează toată activitatea de rețea în conformitate cu reguli de două tipuri: [reguli de rețea pentru aplicații](#) și [reguli pentru pachete de rețea](#).
- **Monitorizare rețea.** Această componentă îți permite să vizualizezi în timp real activitatea de rețea a computerului.
- **Blocare atacuri de rețea.** Această componentă inspectează traficul de rețea la ieșire pentru a detecta activități tipice atacurilor de rețea. Atunci când este detectată o încercare de atac de rețea care are drept țintă calculatorul tău, Kaspersky Endpoint Security blochează activitatea de rețea de la computerul agresor.

Kaspersky Endpoint Security pune la dispoziție următoarele activități:

- **Scanare completă.** Kaspersky Endpoint Security scanează sistemul de operare, inclusiv memoria RAM, obiectele încărcate la pornire, zona de copii de rezervă a sistemului de operare, precum și toate unitățile de hard disk și unitățile amovibile.
- **Scanare particularizată.** Kaspersky Endpoint Security scanează obiectele selectate de utilizator.
- **Scanare zone critice.** Kaspersky Endpoint Security scanează obiectele încărcate la pornirea sistemului de operare, memoria RAM și obiectele vizate de programele rootkit.
- **Actualizare.** Kaspersky Endpoint Security descarcă baze de date actualizate și module actualizate ale aplicației. Actualizarea vă păstrează computerul protejat împotriva celor mai noi virusi și a altor amenințări.
- **Scanare de vulnerabilități.** Kaspersky Endpoint Security scanează sistemul de operare și software-urile instalate pentru detectarea de vulnerabilități. Această scanare asigură detectarea și eliminarea din timp a problemelor potențiale pe care intrușii le pot exploata.

Funcția de criptare a fișierelor îți permite să criptezi fișiere și directoare care sunt stocate pe unități locale ale computerului. Funcția de criptare a unității permite criptarea unităților de hard disk și a unităților amovibile.

## Administrarea la distanță prin aplicația Kaspersky Security Center

Aplicația Kaspersky Security Center face posibilă pornirea și oprirea la distanță a aplicației Kaspersky Endpoint Security, precum și gestionarea și configurarea la distanță a setărilor aplicațiilor.

## Funcții de depanare ale aplicației

Kaspersky Endpoint Security include un număr de funcții de depanare. Funcțiile de depanare sunt acelea de a asigura actualizarea aplicației, de a extinde funcționalitatea ei și de a ajuta utilizatorul în folosirea aplicației.

- **Rapoarte.** În cursul funcționării sale, aplicația ține evidența oricărei componente și activități ale sale creând câte un raport pentru fiecare. Raportul conține lista de evenimente apărute în funcționarea aplicației Kaspersky Endpoint Security și toate operațiunile pe care le efectuează aplicația. În cazul unui incident, poți trimite rapoarte la Kaspersky, unde specialiștii serviciului de asistență vor analiza problema în mod detaliat.
- **Zonă de stocare a datelor.** Dacă aplicația detectează fișiere infectate sau probabil infectate la scanarea computerului în vederea detectării de virusi și alte amenințări, fișierele respective sunt blocate. Kaspersky Endpoint Security mută fișierele probabil infectate într-o zonă de stocare specială denumită *Carantină*. Kaspersky Endpoint Security stochează copiile fișierelor dezinfectate și șterse în *Copii de rezervă*. Kaspersky Endpoint Security mută fișierele neprocesate (indiferent de motiv) în *lista de fișiere neprocesate*. Poți scana fișiere, poți restaura fișiere în directoarele lor inițiale și poți goli zona de stocare a datelor.
- **Serviciul de notificare.** Serviciul de notificare informează utilizatorul despre starea curentă a protecției computerului și despre funcționarea aplicației Kaspersky Endpoint Security. Notificările pot fi afișate pe ecran sau pot fi trimise prin e-mail.
- **Kaspersky Security Network.** Participarea utilizatorilor la Kaspersky Security Network eficientizează protejarea computerelor datorită colectării în timp real de la utilizatori din întreaga lume a unor informații privind reputația fișierelor, a resurselor Web și a software-urilor.
- **Licență.** Achiziționarea unei licențe deblochează funcționalitatea completă a aplicației, oferă acces la actualizările bazei de date și ale modulelor aplicației și asistență prin telefon sau prin e-mail cu privire la instalarea, configurarea și utilizarea aplicației.
- **Asistență.** Toți utilizatorii înregistrați ai aplicației Kaspersky Endpoint Security pot contacta serviciul de asistență tehnică pentru a primi asistență. Poți trimite o solicitare din Contul meu Kaspersky de pe site-ul Web al serviciului de asistență tehnică sau poți primi asistență prin telefon de la personalul de asistență.

Dacă aplicația returnează o eroare sau se blochează în cursul operării, este posibil să repornească automat.

Dacă aplicația întâlnește erori recurente care determină blocarea ei, aplicația efectuează următoarele operațiuni:

1. Dezactivează funcțiile de control și protecție (funcționalitatea de criptare rămâne activată).
2. Îl notifică pe utilizator că funcțiile au fost dezactivate.

3. Încearcă să restabilească starea operațională a aplicației după actualizarea bazelor de date antivirus sau aplicația unor actualizări ale modulelor aplicației.

Aplicația primește informații despre erorile recurente și despre blocările sistemului folosind algoritmi speciali definiți de experți Kaspersky.

## Cerințe hardware și software


Pentru a se asigura funcționarea corectă a aplicației Kaspersky Endpoint Security, computerul trebuie să îndeplinească următoarele cerințe:

Cerințe minime generale:

- 2 GB de spațiu liber pe unitatea de hard disk
- Procesor cu frecvența de 1 GHz (care acceptă setul de instrucțiuni SSE2)
- RAM:
  - 1 GB pentru sistemele de operare pe 32 de biți.
  - 2 GB pentru sistemele de operare pe 64 de biți.

Sisteme de operare acceptate pentru computere personale:


- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 sau o versiune ulterioară;
- Windows 8 Professional/Enterprise;
- Windows 8.1 Professional/Enterprise;
- Windows 10 Home/Pro/Education/Enterprise.

Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows 10, consultă [Baza de cunoștințe a Serviciului de asistență tehnică](#) .

Sisteme de operare acceptate pentru servere de fișiere:

- Windows Small Business Server 2008 Standard/Premium (64 de biți);
- Windows Small Business Server 2011 Essentials/Standard (64 de biți);
- Windows MultiPoint Server 2011 (64 de biți);

- Windows Server 2008 Standard/Enterprise/Datacenter Service Pack 2 sau o versiune ulterioară;
- Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter Service Pack 1 sau o versiune ulterioară;
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter.

Pentru informații detaliate despre asistența pentru sistemele de operare Microsoft Windows Server 2016 și Microsoft Windows Server 2019, consultă [Baza de cunoștințe a Serviciului de asistență tehnică](#) .

## Instalarea și eliminarea aplicației

Această secțiune te îndrumă în procesele de instalare a aplicației Kaspersky Endpoint Security pe computer, de finalizare a configurării inițiale, de efectuare a upgrade-ului de la o versiune anterioară a aplicației și de eliminare a aplicației din computer.

## Instalarea aplicației

Această secțiune descrie cum se instalează Kaspersky Endpoint Security pe computer și cum se finalizează configurarea inițială a aplicației.

## Despre modalitățile de instalare a aplicației

Kaspersky Endpoint Security 10 for Windows poate fi instalat local (direct pe computerul utilizatorului) sau de la distanță, de pe stația de lucru a administratorului.

Instalarea locală a Kaspersky Endpoint Security 10 for Windows poate fi efectuată într-unul din modurile următoare:

- În mod interactiv, folosind Expertul de configurare a aplicației.  
Modul interactiv necesită implicarea ta directă în procesul de instalare.
- În modul silențios, [din linia de comandă](#).  
După pornirea instalării în modul silențios, nu este nevoie de implicarea ta în procesul de instalare.

Aplicația poate fi instalată de la distanță pe computere din rețea folosind următoarele:

- suita software Kaspersky Security Center (consultă *Ghidul de instalare Kaspersky Security Center*).
- Editorul de politică de grup din Microsoft Windows (vezi fișierele de ajutor din sistemul de operare).
- [System Center Configuration Manager](#).

Recomandăm închiderea tuturor aplicațiilor în execuție înainte de a începe instalarea Kaspersky Endpoint Security (inclusiv instalarea la distanță).

## Instalarea aplicației folosind Expertul de instalare

Interfața aplicației Expert de configurare constă dintr-o secvență de ferestre corespunzătoare pașilor de instalare a aplicației. Poți naviga între paginile Expertului de instalare folosind butoanele **Înapoi** și **Următorul**. Pentru a închide Expertul de instalare după finalizarea activității, fă clic pe butonul **Terminare**. Pentru a opri Expertul de instalare în orice fază, fă clic pe butonul **Revocare**.

*Pentru a instala aplicația sau pentru a efectua un upgrade al aplicației de la o versiune anterioară folosind Expertul de instalare:*

1. Execută fișierul setup.exe inclus în [kitul de distribuire](#).

Expertul de instalare pornește.

2. Urmează instrucțiunile din Expertul de instalare.

După lansarea fișierului setup.exe, Kaspersky Endpoint Security verifică dacă pe computer există software-uri incompatibile. În mod implicit, după detectarea de software-uri incompatibile, procesul de instalare este abandonat și pe ecran apare lista de aplicații incompatibile cu aplicația Kaspersky Endpoint Security. Pentru a continua instalarea, elimină aceste aplicații de pe computer.

## Pasul 1. Cum să te asiguri că îndeplinește computerul cerințele de instalare

Înainte de a instala Kaspersky Endpoint Security 10 pentru Windows pe un computer sau de a actualiza o versiune anterioară a aplicației, trebuie verificate următoarele condiții:

- Sistemul de operare și pachetul Service Pack îndeplinesc [cerințele software pentru instalarea produsului](#).
- Sunt sau nu îndeplinite [cerințele hardware și software](#).

- Dacă utilizatorul are sau nu drepturile de a instala produsul software.

Dacă nu sunt îndeplinite toate cerințele anterioare, o notificare relevantă este afișată pe ecran.

Dacă sunt îndeplinite condițiile prezentate, Expertul de instalare caută aplicații Kaspersky care ar putea conduce la conflicte atunci când sunt executate în același timp cu aplicația care este instalată. Dacă sunt găsite astfel de aplicații, ți se solicită eliminarea lor manuală.

Dacă aplicațiile detectate includ versiuni anterioare de Kaspersky Endpoint Security, toate datele care pot fi migrate (cum ar fi datele de activare și setările pentru aplicații) sunt reținute și utilizate la instalarea Kaspersky Endpoint Security 10 Service Pack 2 for Windows, iar versiunea anterioară a aplicației este eliminată automat. Acest lucru este aplicabil pentru următoarele versiuni ale aplicației:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

## Pasul 2. Pagina de Bun venit pentru procedura de instalare

Dacă sunt îndeplinite toate cerințele pentru instalarea aplicației, apare un mesaj de bun venit după pornirea pachetului de instalare. Pagina de Bun venit te anunță de pornirea instalării Kaspersky Endpoint Security pe computer.

Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**.

## Pasul 3. Vizualizarea Acordului de licență

În acest pas ești sfătuit să vezi acordul de licență dintre tine și Kaspersky.

Citește cu atenție acordul și, dacă accepți toți termenii săi, bifează caseta de selectare **Accept termenii acordului de licență**.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 4. Selectarea tipului de instalare

În acest pas poți selecta cel mai potrivit tip de instalare pentru Kaspersky Endpoint Security:

- **Instalare de bază.** Dacă alegi acest tip de instalare, vor fi instalate pe computer componentele protecției, Control drepturi aplicații și Monitor de vulnerabilități, cu setările recomandate de experții Kaspersky.
- **Instalare standard.** Dacă alegi acest tip de instalare, pe computer sunt instalate numai componentele de protecție și de control cu setările recomandate de Kaspersky.
- **Instalare particularizată.** Dacă alegi acest tip de instalare, ți se va solicita să selectezi [componentele de instalat](#) și să specifici [directorul de destinație pentru aplicație](#).

Acest tip de instalare îți permite instalarea componentelor care nu sunt incluse în instalările de bază și standard.

Instalarea standard este selectată în mod implicit.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 5. Selectarea componentelor aplicației de instalat

Acest pas este efectuat dacă selectezi *Instalare particularizată* pentru aplicație.

În acest pas poți selecta componentele Kaspersky Endpoint Security pe care dorești să le instalezi. Instalarea componentei Antivirus pentru fișiere este obligatorie. Nu poți anula instalarea ei.

În mod implicit sunt selectate spre instalare toate componentele aplicației, cu excepția următoarelor:

- [Prevenire atac BadUSB](#).
- [Criptare unitate](#).
- [Criptare fișiere](#).
- [Gestionare Microsoft BitLocker](#).
- [Senzor KATA Endpoint](#).

*Gestionare Microsoft BitLocker* efectuează următoarele funcții:

- Administrează criptarea BitLocker încorporată în sistemul de operare Windows.



- Configurează setările politicii de criptare și verifică aplicabilitatea lor pentru computerul administrat.
- Începe procesele de criptare și decriptare.
- Monitorizează starea criptării pe computerul administrat.
- Stochează centralizat cheile de recuperare pe Serverul de administrare Kaspersky Security Center.

*Senzorul KATA Endpoint* este o componentă a Kaspersky Anti Targeted Attack Platform. Această soluție este destinată detectării rapide a amenințărilor de tipul atacurilor țintite. Componenta monitorizează continuu procese, conexiuni de rețea active și fișiere care sunt modificate și transmite aceste informații către Kaspersky Anti Targeted Attack Platform.

Pentru a selecta o componentă de instalat, fă clic pe pictograma de lângă numele componentei pentru a afișa meniul contextual și selectează **Această caracteristică va fi instalată pentru a se executa de pe discul local**. Pentru detalii despre ce activități sunt efectuate de componenta selectată și cât spațiu-disc este necesar pentru a instala componenta, consultă partea inferioară a paginii Expert de instalare.

Pentru a vedea informații detaliate despre spațiul disponibil pe unitățile locale de hard disk, fă clic pe butonul **Volum**. Informațiile vor fi afișate în fereastra **Spațiu-disc disponibil** care se deschide.

Pentru a anula instalarea componentei, selectează opțiunea **Caracteristica va fi indisponibilă** în meniul contextual.

Pentru a reveni la lista de componente instalate în mod implicit, fă clic pe butonul **Reinițializare**.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 6. Selectarea directorului de destinație

Acest pas este disponibil dacă selectezi *Instalare particularizată* pentru aplicație.

În acest pas poți specifica pentru directorul de destinație calea în care va fi instalată aplicația. Pentru a selecta directorul de destinație pentru aplicație, fă clic pe butonul **Răsfoire**.

Pentru a vedea informații despre spațiul disponibil pe unitățile locale de hard disk, fă clic pe butonul **Volum**. Informația este afișată în fereastra **Cerințe de spațiu-disc** care se deschide.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 7. Adăugarea de excluderi de la scanarea de viruși

Acest pas este disponibil dacă selectezi *Instalare particularizată* pentru aplicație.

În această etapă poți specifica excluderile de la scanarea de viruși pe care dorești să le adaugi în setările aplicației.

Casetele de selectare **Exclude din domeniul de scanare de viruși zone recomandate de Microsoft** / **Exclude din domeniul de scanare de viruși zone recomandate de Kaspersky** exclud zonele recomandate de Microsoft și, respectiv, de Kaspersky din zona de încredere sau le include.

Dacă una dintre aceste casete de selectare este bifată, Kaspersky Endpoint Security include în zona de încredere zonele pe care le recomandă Microsoft sau Kaspersky. Kaspersky Endpoint Security nu scanează aceste zone de viruși sau alte amenințări.

Caseta de selectare **Exclude din domeniul de scanare de viruși zone recomandate de Microsoft** este disponibilă atunci când Kaspersky Endpoint Security este instalat pe un computer pe care se execută Microsoft Windows pentru servere de fișiere.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 8. Pregătirea instalării aplicației

Îți recomandăm să protejezi procesul de instalare, deoarece computerul tău este posibil să fi fost infectat cu programe periculoase care ar putea interfera cu instalarea Kaspersky Endpoint Security 10 for Windows.

Protecția procesului de instalare este activată în mod implicit.

Dacă însă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare. În acest caz, abandonează instalarea și repornește Expertul de instalare a aplicației. La pasul „Pregătirea instalării aplicației”, debifează caseta de selectare **Protejare proces de instalare**.

Caseta de selectare **Asigură compatibilitatea cu serviciile de asigurare acces Citrix** activează/dezactivează funcția care instalează drivere în modul de compatibilitate Citrix PVS.

Bifează această casetă de selectare dacă lucrezi cu Citrix Provisioning Services.

Caseta de selectare **Adaugă calea către fișierul avp.com la variabila de sistem %PATH%** activează/dezactivează o opțiune care adaugă calea către fișierul avp.com la variabila de sistem %PATH%.

Dacă această casetă de selectare este bifată, lansarea Kaspersky Endpoint Security sau a uneia dintre activitățile sale din linia de comandă nu necesită introducerea căii către fișierul executabil. Este suficient să introduci numele fișierului executabil și comanda de a începe activitatea particulară.

Pentru a reveni la pasul precedent al Expertului de instalare, fă clic pe butonul **Înapoi**. Pentru a instala programul, fă clic pe butonul **Instalare**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

Conexiunile de rețea curente pot fi terminate cât timp aplicația este instalată pe computer. Majoritatea conexiunilor de rețea terminate sunt restabilite după finalizarea instalării aplicației.

## Pasul 9. Instalarea aplicației

Instalarea aplicației poate dura ceva timp. Așteaptă finalizarea ei.

Dacă actualizezi aplicația de la o versiune anterioară, acest pas include și migrarea setărilor și eliminarea versiunii anterioare a aplicației.

După finalizarea instalării Kaspersky Endpoint Security, pornește [Expertul de configurare inițială](#).

## Instalarea aplicației din linia de comandă

Aplicația Kaspersky Endpoint Security poate fi instalată din linia de comandă într-unul din următoarele moduri:

- În mod interactiv, folosind Expertul de configurare a aplicației.
- În modul silențios. După pornirea instalării în modul silențios, nu este nevoie de implicarea ta în procesul de instalare. Pentru a instala aplicația în modul silențios, utilizează `/s` și `/qn`.

*Pentru a instala aplicația sau a face upgrade pentru versiunea aplicației:*

1. Execută interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.

## 3. Execută următoare comandă:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0]
[/pADDLOCAL=<componentă>] [/pSKIPPRODUCTCHECK=1|0]
[/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<nume utilizator> /pKLPASSWD=
<parolă> /pKLPASSWDAREA=<domeniu parolă>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<nivel urmărire>] /s
```

sau

```
msiexec /i <nume kit distribuție> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1|0] [ADDLOCAL=<componentă>] [SKIPPRODUCTCHECK=1|0]
[SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nume utilizator> KLPASSWD=<parolă>
KLPASSWDAREA=<domeniu parolă>] [ENABLETRACES=1|0 TRACESLEVEL=<nivel
urmărire>] /qn
```

## EULA

Acceptarea sau refuzarea termenilor Acordului de licență pentru utilizatorul final. Valori disponibile:

- 1 – acceptarea termenilor Acordului de licență pentru utilizatorul final.
- 0 – refuzarea termenilor Acordului de licență pentru utilizatorul final.  
Textul Acordului de licență este inclus în [kitul de distribuire al Kaspersky Endpoint Security](#). Acceptarea termenilor Acordului de licență pentru utilizatorul final este necesară pentru instalarea aplicației sau pentru efectuarea unui upgrade la versiunea aplicației.

## PRIVACYPOLICY

Acceptarea sau refuzarea Politicii de confidențialitate. Valori disponibile:

- 1 – acceptarea Politicii de confidențialitate.
- 0 – refuzarea Politicii de confidențialitate.  
Textul Politicii de confidențialitate este inclus în [kitul de distribuire Kaspersky Endpoint Security](#). Pentru a instala aplicația sau pentru a face upgrade la versiunea aplicației, trebuie să accepți Politica de confidențialitate.

**KSN**

Acordul sau refuzul de a participa în Kaspersky Security Network. Dacă pentru acest parametru nu este setată nicio valoare, Kaspersky Endpoint Security îți va solicita să confirmi consimțământul sau refuzul de a participa la KSN la prima pornire a aplicației Kaspersky Endpoint Security. Valori disponibile:

- 1 – acord de participare la KSN.
- 0 – refuz de a participa la KSN (valoare implicită).

Pachetul de distribuție Kaspersky Endpoint Security este optimizat pentru utilizare cu Kaspersky Security Network. Dacă ai optat să nu participi la Kaspersky Security Network, ar trebui să îți actualizezi Kaspersky Endpoint Security imediat după finalizarea instalării.

**ALLOWREBOOT=1**

Se repornește automat computerul dacă este necesar după instalarea sau upgrade-ul aplicației. Dacă nu este setată nicio valoare pentru acest parametru, repornirea automată a computerului este blocată.

Repornirea nu este necesară atunci când instalați Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să eliminați aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizați versiunea aplicației.

**ADDLOCAL**

Selectați componente suplimentare pentru instalare. În mod implicit, toate componentele aplicației sunt selectate pentru instalare, cu excepția următoarelor componente: BadUSB Attack Prevention, File Level Encryption, Full Disk Encryption, BitLocker Management și KATA Endpoint Sensor. Valori disponibile:

- MSBitLockerFeature. Componenta BitLocker Manager este instalată.
- AntiAPTFeature. Este instalată componenta Senzor KATA Endpoint.

**SKIPPRODUCTCHECK=1**

Dezactivarea verificării existenței programelor software incompatibile. Lista programelor software incompatibile este disponibilă în fișierul incompatible.txt, care este inclus în [kitul de distribuție](#). Dacă nu este setată nicio valoare pentru acest parametru și este detectat un software, instalarea aplicației Kaspersky Endpoint Security va fi oprită.

**SKIPPRODUCTUNINSTALL=1**

Dezactivarea eliminării automate a programelor software incompatibile detectate. Dacă nu este setată nicio valoare pentru acest parametru, Kaspersky Endpoint Security încearcă să elimine software-ul incompatibil.

**KLLOGIN**

Setează numele de utilizator pentru accesarea caracteristicilor și setărilor aplicației Kaspersky Endpoint Security (componenta [Protecție prin parolă](#)). Numele de utilizator se setează împreună cu setările KLPASSWD și KLPASSWDAREA. Numele de utilizator implicit este KLAdmin.

**KLPASSWD**

Specifică o parolă pentru accesarea funcțiilor și setărilor Kaspersky Endpoint Security (parola este specificată împreună cu parametrii KLLOGIN și KLPASSWDAREA).

Dacă ai specificat o parolă, însă nu ai specificat un număr de utilizator cu parametrul KLLOGIN, se utilizează în mod implicit numele de utilizator KLAdmin.

**KLPASSWDAREA**

Specifică domeniul parolei pentru accesarea aplicației Kaspersky Endpoint Security. Atunci când un utilizator încearcă să efectueze o acțiune care este inclusă în acest domeniu, Kaspersky Endpoint Security solicită utilizatorului acreditările contului (parametrii KLLOGIN și KLPASSWD). Folosește caracterul „;” pentru a specifica mai multe valori. Valori disponibile:

- SET – modificare a setărilor aplicației.
- EXIT – ieșire din aplicație.

- **DISPROTECT** – dezactivarea componentelor protecției și oprire a activităților de scanare.
- **DISPOLICY** – dezactivarea politicii Kaspersky Security Center.
- **UNINST** – eliminarea aplicației de pe computer.
- **DISCTRL** – dezactivare a componentelor de control.
- **REMOVELIC** – eliminare a cheii.
- **REPORTS** – vizualizarea rapoartelor.

**ENABLETRACES**

Activarea sau dezactivarea urmăririi aplicațiilor. După ce Kaspersky Endpoint Security pornește, acesta salvează fișierele de urmărire în directorul %ProgramData%/Kaspersky Lab. Valori disponibile:

- **1** – urmărirea este activată.
- **0** – urmărirea este dezactivată (valoare implicită).

**TRACESLEVEL**

Nivelul de detaliere a urmăririi. Valori disponibile:

- **100** (critic). Numai mesajele de eroare critice.
- **200** (ridicat). Mesaje despre toate erorile, inclusiv erorile fatale.
- **300** (diagnosticare). Mesaje despre toate erorile și o selecție de mesaje care conțin avertizări.
- **400** (important). Toate avertizările și mesajele despre erorile obișnuite și cele critice, precum și o selecție de mesaje care conțin informații suplimentare.

- **500 (normal).** Toate avertismentele și mesajele despre erorile obișnuite și cele critice, precum și mesajele cu informații detaliate despre funcționarea aplicației în modul normal (valoare implicită).
- **600 (scăzut).** Toate mesajele posibile.

Exemplu:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pALLOWREBOOT=1 /s  
  
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1  
KLLOGIN=Admin KLPASSWD=Password  
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn  
  
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

După instalarea aplicației, Kaspersky Endpoint Security activează licența de probă, cu excepția cazului în care ai indicat un cod de activare în [fișierul setup.ini](#). O licență trial are, de obicei, un termen scurt. După expirarea licenței trial, toate caracteristicile aplicației Kaspersky Endpoint Security sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie [să activezi o licență comercială](#).

Atunci când instalezi aplicația sau efectuezi upgrade versiunii aplicației în modul silențios, este acceptată folosirea următoarelor fișiere:

- [setup.ini](#) – setări generale de configurare a aplicației;
- [install.cfg](#) – setări locale ale Kaspersky Endpoint Security;
- setup.reg – chei de registru.

Cheile de registru din fișierul setup.reg se scriu în registru numai dacă valoarea setup.reg este setată pentru parametrul SetupReg în fișierul setup.ini. Fișierul setup.reg este generat de experții de la Kaspersky. Nu este recomandabilă modificarea conținutului acestui fișier.

Pentru a aplica setări din fișierul setup.ini și setup.reg, plasează aceste fișiere în directorul care conține pachetul de distribuție Kaspersky Endpoint Security.



# Instalarea la distanță a aplicației folosindu-se System Center Configuration Manager

Aceste instrucțiuni se aplică pentru System Center Configuration Manager 2012 R2.

*Pentru a instala la distanță o aplicație folosind System Center Configuration Manager:*

1. Deschide consola Configuration Manager.
2. În dreapta consolei, în secțiunea **Gestionare aplicații**, selectează **Pachete**.
3. În partea de sus a consolei, în panoul de control, fă clic pe butonul **Creare pachet**.  
Este lansat *Expert pachet nou și aplicație*.

4. În Expert pachet nou și aplicație:

a. În secțiunea **Pachet**:

- În câmpul **Nume**, introdu numele pachetului de instalare.
- În câmpul **Director sursă**, specifică o cale către directorul care conține kitul de distribuție pentru Kaspersky Endpoint Security.

b. În secțiunea **Tip aplicație**, selectează opțiunea **Aplicație standard**.

c. În secțiunea **Aplicație standard**:

- În câmpul **Nume**, introdu numele unic pentru pachetul de instalare (de exemplu, numele aplicației, inclusiv versiunea).
- În câmpul **Linie de comandă**, specifică opțiunile de instalare din linia de comandă pentru Kaspersky Endpoint Security.
- Fă clic pe butonul **Răsfoire** pentru a introduce o cale către fișierul executabil al aplicației.
- Asigură-te că lista **Mod de executare** are selectat elementul **Executare cu drepturi de administrator**.

d. În secțiunea **Cerințe**:

- Bifează caseta de selectare **Pornește altă aplicație mai întâi** dacă dorești ca o altă aplicație să fie lansată înainte de a instala Kaspersky Endpoint Security.

Selectează aplicația din lista verticală **Aplicație** sau specifică o cale către fișierul executabil al acestei aplicații făcând clic pe butonul **Răsfoire**.

- Selectează opțiunea **Această aplicație poate fi pornită numai pe platformele specificate** în secțiunea **Cerințe platformă**, dacă dorești ca aplicația să fie instalată numai pe sistemele de operare specificate.

În lista de mai jos, bifează casetele de selectare de lângă sistemele de operare pe care va fi instalat Kaspersky Endpoint Security.

Acest pas este opțional.

- e. În secțiunea **Sumar**, verifică toate valorile introduse pentru setări și fă clic pe **Următorul**.

Pachetul de instalare creat va apărea în secțiunea **Pachete**, în lista de pachete de instalare disponibile.

5. În meniul contextual al pachetului de instalare, selectează **Implementare**.

Această acțiune pornește *Expertul de implementare*.

6. În Expertul de implementare:

- a. În secțiunea **General**:

- În câmpul **Software**, introdu numele unic al pachetului de instalare sau selectează pachetul de instalare din listă făcând clic pe butonul **Răsfoire**.
- În câmpul **Colecție**, introdu numele colecției de computere pe care va fi instalată aplicația sau selectează colecția făcând clic pe butonul **Răsfoire**.

- b. În secțiunea **Conține**, adaugă puncte de distribuție (pentru informații mai detaliate, consultă documentația de ajutor pentru System Center Configuration Manager).

- c. Dacă este nevoie, specifică valorile pentru alte setări în Expertul de implementare. Aceste setări sunt opționale pentru instalarea la distanță a Kaspersky Endpoint Security.

- d. În secțiunea **Sumar**, verifică toate valorile introduse pentru setări și fă clic pe **Următorul**.

După finalizarea Expertului de implementare, va fi creată o activitate pentru instalarea la distanță a Kaspersky Endpoint Security.

## Descrierea setărilor fișierului setup.ini

Fișierul setup.ini este folosit atunci când se instalează aplicația din linia de comandă sau se folosește Editorul de politică de grup al Microsoft Windows. Pentru a aplica setări din fișierul setup.ini, plasează acest fișier în directorul care conține pachetul de distribuție Kaspersky Endpoint Security.

Fișierul setup.ini constă din următoarele secțiuni:

- [Setup] – opțiuni generale de instalare a aplicației.
- [Components] – selecția componentelor de aplicație de instalat. Dacă niciuna dintre componente nu este specificată, sunt instalate toate componentele disponibile pentru sistemul de operare. Antivirus pentru fișiere este o componentă obligatorie și se instalează pe computer indiferent care setări sunt indicate în această secțiune.
- [Tasks] – selecție a activităților care vor fi incluse în lista de activități Kaspersky Endpoint Security. Dacă nu este specificată nicio activitate, sunt incluse toate activitățile din lista de activități a Kaspersky Endpoint Security.

Valorile alternative pentru valoarea 1 sunt yes, on, enable și enabled.

Valorile alternative pentru valoarea 0 sunt no, off, disable și disabled.

Setări ale fișierului setup.ini file

Secțiune	Parametru	Descriere
[Setup]	InstallDir	Calea către directorul de instalare a aplicației.
	ActivationCode	Codul de activare pentru Kaspersky Endpoint Security.
	Eula	<p>Acceptarea sau refuzarea termenilor Acordului de licență pentru utilizatorul final. Valori disponibile:</p> <ul style="list-style-type: none"> <li>• 1 – acceptarea termenilor Acordului de licență pentru utilizatorul final.</li> <li>• 0 – refuzarea termenilor Acordului de licență pentru utilizatorul final.</li> </ul>

Textul Acordului de licență este inclus în [kitul de distribuire al Kaspersky Endpoint Security](#).

Acceptarea termenilor Acordului de licență pentru utilizatorul final este necesară pentru instalarea aplicației sau pentru efectuarea unui upgrade la versiunea aplicației.

## PrivacyPolicy

Acceptarea sau refuzarea Politicii de confidențialitate. Valori disponibile:

- 1 – acceptarea Politicii de confidențialitate.
- 0 – refuzarea Politicii de confidențialitate.

Textul Politicii de confidențialitate este inclus în [kitul de distribuire Kaspersky Endpoint Security](#). Pentru a instala aplicația sau pentru a face upgrade la versiunea aplicației, trebuie să acceptți Politica de confidențialitate.

## KSN

Acordul sau refuzul de a participa în Kaspersky Security Network. Dacă pentru acest parametru nu este setată nicio valoare, Kaspersky Endpoint Security îți va solicita să confirmi consimțământul sau refuzul de a participa la KSN la prima pornire a aplicației Kaspersky Endpoint Security. Valori disponibile:

- 1 – acord de participare la KSN.
- 0 – refuz de a participa la KSN (valoare implicită).

Pachetul de distribuție Kaspersky Endpoint Security este optimizat pentru utilizare cu Kaspersky Security Network. Dacă ai optat să nu participi la Kaspersky Security Network, ar trebui să îți actualizezi Kaspersky Endpoint Security imediat după finalizarea instalării.

### Login

Setează numele de utilizator pentru accesarea caracteristicilor și setărilor aplicației Kaspersky Endpoint Security (componenta  [Protecție prin parolă](#) ). Numele de utilizator se setează împreună cu setările Password și PasswordArea. Numele de utilizator implicit este KLAdmin.

### Password

Specifică o parolă pentru accesarea funcțiilor și setărilor Kaspersky Endpoint Security (parola este specificată împreună cu parametrii Login și PasswordArea).

Dacă ai specificat o parolă, însă nu ai specificat un număr de utilizator cu parametrul Conectare, se utilizează în mod implicit numele de utilizator KLAdmin.

### PasswordArea

Specifică domeniul parolei pentru accesarea aplicației Kaspersky Endpoint Security. Atunci când un utilizator încearcă să efectueze o acțiune care este inclusă în acest domeniu, Kaspersky Endpoint Security solicită utilizatorului acreditările contului (parametrii Nume de conectare și Parolă). Folosește caracterul „;” pentru a specifica mai multe valori. Valori disponibile:

- SET – modificare a setărilor aplicației.
- EXIT – ieșire din aplicație.
- DISPROTECT – dezactivarea componentelor protecției și oprire a activităților de scanare.
- DISPOLICY – dezactivarea politicii Kaspersky Security Center.
- UNINST – eliminarea aplicației de pe computer.
- DISCTRL – dezactivare a componentelor de control.
- REMOVELIC – eliminare a cheii.
- REPORTS – vizualizarea rapoartelor.

### SelfProtection

Activează sau dezactivează mecanismul de protecție a instalării aplicației. Valori disponibile:

- 1 – mecanismul de protecție a instalării aplicației este activat.
- 0 – mecanismul de protecție a instalării aplicației este dezactivat.

Poți dezactiva protejarea instalării. Protejarea instalării include protecția împotriva falsificării pachetului de distribuție cu programe malware, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea registry de sistem care conține cheile aplicației. Dacă însă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare.

#### Reboot=1

Se repornește automat computerul dacă este necesar după instalarea sau upgrade-ul aplicației. Dacă nu este setată nicio valoare pentru acest parametru, repornirea automată a computerului este blocată.

Repornirea nu este necesară atunci când instalați Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să eliminați aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizați versiunea aplicației.

#### AddEnvironment

La variabila de sistem %PATH% adăugați calea către fișierele executabile localizate în directorul de instalare Kaspersky Endpoint Security. Valori disponibile:

- 1 – la variabila de sistem %PATH% se adaugă calea către fișierele executabile localizate în directorul de

instalare pentru Kaspersky Endpoint Security.

- 0 – la variabila de sistem %PATH% nu se adaugă calea către fișierele executabile localizate în directorul de instalare pentru Kaspersky Endpoint Security.

#### AMPPL

Activează sau dezactivează protecția serviciului Kaspersky Endpoint Security folosind tehnologia AM-PPL (Antimalware Protected Process Light). Valori disponibile:

- 1 – protecția serviciului Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este activată.
- 0 – protecția serviciului Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este dezactivată.

#### SetupReg

Activează scrierea de chei de registru din fișierul setup.reg în registru. Valoarea parametrului SetupReg: setup.reg.



## EnableTraces

Activarea sau dezactivarea urmării instalării aplicației. Kaspersky Endpoint Security salvează fișierele de urmărire în directorul %ProgramData%/Kaspersky Lab. Valori disponibile:

- 1 – urmărirea instalării aplicației este activată.
- 0 – urmărirea instalării aplicației este dezactivată (valoare implicită).

## TracesLevel

Nivelul de detaliere a urmării. Valori disponibile:

- 100 (critic). Numai mesajele de eroare critice.
- 200 (ridicat). Mesaje despre toate erorile, inclusiv erorile fatale.
- 300 (diagnosticare). Mesaje despre toate erorile și o selecție de mesaje care conțin avertizări.
- 400 (important). Toate avertizările și mesajele despre erorile obișnuite și cele critice, precum și o selecție de mesaje care conțin informații suplimentare.
- 500 (normal). Toate avertismentele și mesajele despre erorile obișnuite și cele critice, precum și mesajele cu informații detaliate despre funcționarea aplicației în modul normal (valoare implicită).

- 600 (scăzut). Toate mesajele posibile.

[Components]	ALL	Instalați toate componentele. Dacă este specificată valoarea 1 pentru acest parametru, vor fi instalate toate componentele, indiferent de setările de instalare ale componentelor individuale.
	MailAntiVirus	Antivirus pentru e-mail.
	IMAntiVirus	Antivirus IM.
	WebAntiVirus	Antivirus pentru Web.
	ApplicationPrivilegeControl	Componenta Control privilegii aplicații.
	SystemWatcher	Monitorizare sistem.
	Firewall	Firewall.
	NetworkAttackBlocker	Blocare atacuri de rețea.
	WebControl	Control Web.
	DeviceControl	Componenta Control dispozitive.
	ApplicationStartupControl	Componenta Control pornire aplicații.
	FileEncryption	Biblioteci File Level Encryption.
	DiskEncryption	Biblioteci Full Disk Encryption.
	VulnerabilityAssessment	Monitor de vulnerabilități.
	KeyboardAuthorization	Prevenire atac BadUSB.
	AntiAPT	Senzor Kata Endpoint.
	MSBitLocker	Gestionare Microsoft BitLocker.
	AdminKitConnector	<p><a href="#">Conector agent de rețea</a> pentru administrare la distanță a aplicației prin Kaspersky Security Center. Valori disponibile:</p> <ul style="list-style-type: none"> <li>• 1 – componenta Conector agent de rețea este instalată.</li> </ul>

- 0 – componenta Conector agent de rețea nu este instalată.

[Tasks]

## ScanMyComputer

Activitate de scanare completă.

Valori disponibile:

- 1 – activitatea este inclusă în lista de activități Kaspersky Endpoint Security.
- 0 – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.

## ScanCritical

Activitate de scanare a zonelor critice. Valori disponibile:

- 1 – activitatea este inclusă în lista de activități Kaspersky Endpoint Security.
- 0 – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.

## Updater

Activitate de actualizare. Valori disponibile:

- 1 – activitatea este inclusă în lista de activități Kaspersky Endpoint Security.
- 0 – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.

Expertul de configurare inițială

Expertul de configurare inițială al Kaspersky Endpoint Security pornește la sfârșitul procedurii de instalare a aplicației. Expertul de configurare inițială îți permite să activezi aplicația și să aduni informații despre aplicațiile incluse în sistemul de operare. Aceste aplicații sunt adăugate la lista de aplicații de încredere ale căror acțiuni în interiorul sistemului de operare nu sunt supuse niciunor restricții.

Interfața Expertului de configurare inițială constă într-o secvență de pagină (pași). Poți naviga între paginile Expertului de configurare inițială folosind butoanele **Înapoi** și **Următorul**. Pentru a finaliza procedura Expertului de configurare inițială, fă clic pe butonul **Terminare**. Pentru a opri Expertul de configurare inițială în orice moment, fă clic pe **Revocare**.

Dacă Expertul de configurare inițială este întrerupt dintr-un motiv oarecare, setările deja specificate nu sunt salvate. La următoarea tentativă de folosire a aplicației, Expertul de configurare inițială va porni din nou și va trebui să configureze setările de la început.

## Activarea aplicației

Aplicația trebuie să fie activată pe un computer pe care data și ora sistemului sunt actuale. Dacă data și ora sistemului sunt modificate după activarea aplicației, cheia devine inoperabilă. Aplicația trece într-un mod de operare fără actualizări, iar Kaspersky Security Network nu va fi disponibil. Cheia poate redeveni operabilă din nou după reinstalarea sistemului de operare.

În acest pas selectează una dintre următoarele opțiuni de activare Kaspersky Endpoint Security:

- **Activare cu un cod de activare.** Pentru a activa aplicația folosind un [cod de activare](#), selectează această opțiune și introdu un cod de activare.
- **Activare cu un fișier cheie.** Selectează această opțiunea pentru a activa aplicația cu un fișier cheie.
- **Activare versiune trial.** Selectează această opțiune pentru a activa versiunea trial a aplicației. Utilizatorul poate folosi versiunea complet funcțională a aplicației pe durata termenului limitat de licență pentru versiunea trial a aplicației. După expirarea licenței, funcționalitatea aplicației este blocată și nu poți activa din nou versiunea trial.
- **Activare ulterioară.** Selectează această opțiune dacă dorești să treci peste etapa de activare a Kaspersky Endpoint Security. Utilizatorul va putea să lucreze numai cu componentele Antivirus pentru fișiere și Firewall. Utilizatorul va putea actualiza bazele de date antivirus și modulele Kaspersky Endpoint Security o singură dată după instalare. Opțiunea **Activare ulterioară** este disponibilă numai la prima pornire a Expertului de configurare inițială, imediat după instalarea aplicației.

Este necesară o conexiune Internet pentru a activa versiunea trial a aplicației sau pentru a activa aplicația folosind un cod de activare.

Pentru a continua Expertul de configurare inițială, selectează o opțiune de activare și fă clic pe butonul **Următorul**. Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Activarea cu un cod de activare

Acest pas este disponibil atunci când îți activezi aplicația cu un cod de activare. Acest pas este omis atunci când activezi versiunea trial a aplicației sau atunci când activezi aplicația cu un fișier cheie.

În acest pas, Kaspersky Endpoint Security trimite date către serverul de activare pentru a verifica acest cod de activare introdus:

- Dacă verificarea codului de activare se face cu succes, Expertul de configurare inițială continuă automat cu fereastra următoare.
- Dacă verificarea codului de activare nu reușește, apare un mesaj corespunzător. În acest caz, ar trebui să soliciți sfatul distribuitorului de software de la care ai achiziționat licența Kaspersky Endpoint Security.
- Dacă este depășit numărul de activări pentru acest cod de activare, apare o notificare corespunzătoare. Expertul de configurare inițială este întrerupt și aplicația sugerează contactarea asistenței tehnice Kaspersky Lab.

Pentru a reveni la pasul precedent al Expertului de configurare inițială, fă clic pe butonul **Înapoi**. Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Activarea utilizând un fișier cheie

Acest pas este disponibil numai atunci când îți activezi aplicația cu un fișier cheie.

În acest pas, precizează calea către fișierul cheie. Pentru aceasta, fă clic pe butonul **Răsfoire** și selectează un fișier cheie care are forma <ID fișier>.key.

După ce selectezi un fișier cheie, sunt afișate următoarele informații în partea de jos a ferestrei:

- Cheie
- Tip licență (comercială sau trial) și numărul de computere care sunt acoperite de această licență
- Data activării aplicației pe computer
- Dată expirare licență
- Funcționalitatea aplicației disponibilă în baza licenței
- Notificări despre problemele legate de cheie, dacă este cazul. De exemplu, *Lista neagră de chei este coruptă*.

Pentru a reveni la pasul precedent al Expertului de configurare inițială, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de configurare inițială, fă clic pe butonul **Următorul**. Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Selectarea funcțiilor de activat

Acest pas este disponibil numai atunci când activezi versiunea trial a aplicației.

În acest pas poți selecta funcționalitatea care va deveni disponibilă după activarea aplicației:

- **Instalare de bază.** Dacă este selectată această opțiune, după activarea aplicației vor fi disponibile numai componentele de protecție, Control drepturi aplicații și Monitor de vulnerabilități.
- **Instalare standard.** Dacă este selectată această opțiune, după activare vor fi disponibile numai componentele de protecție și control ale aplicației.
- **Instalare completă.** Dacă este selectată această opțiune, după activarea aplicației vor fi disponibile toate componentele instalate ale aplicației, inclusiv funcționalitatea de criptare a datelor.

Dacă în cursul instalării ai selectat mai multe componente decât permite licența achiziționată, după activarea aplicației componentele care nu sunt disponibile în baza licenței vor rămâne instalate, dar nu vor fi operaționale. Dacă licența achiziționată permite folosirea mai multor componente decât cele instalate în mod curent, după activarea aplicației componentele care nu au fost instalate vor fi listate în secțiunea **Licențiere**.

Instalarea standard este selectată în mod implicit.

Pentru a reveni la pasul precedent al Expertului de configurare inițială, fă clic pe butonul **Înapoi**. Pentru a lansa Expertul de configurare inițială, fă clic pe butonul **Următorul**. Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Finalizarea activării

În acest pas, Expertul de configurare inițială te informează despre activarea cu succes a Kaspersky Endpoint Security. Sunt furnizate următoarele informații despre licență:

- Tip licență (comercială sau trial) și numărul de computere care sunt acoperite de această licență
- Dată expirare licență
- Funcționalitatea aplicației disponibilă în baza licenței

Pentru a lansa Expertul de configurare inițială, fă clic pe butonul **Următorul**. Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Analizarea sistemului de operare

În acest pas sunt colectate informații despre aplicațiile incluse în sistemul de operare. Aceste aplicații sunt adăugate la lista de aplicații de încredere ale căror acțiuni în interiorul sistemului de operare nu sunt supuse niciunor restricții.

Celelalte aplicații sunt analizate când sunt pornite pentru prima dată, după instalarea Kaspersky Endpoint Security.

Pentru a opri Expertul de configurare inițială, fă clic pe butonul **Revocare**.

## Finalizarea configurării inițiale a aplicației

Fereastra de finalizare a Expertului de configurare inițială conține informații despre finalizarea procesului de instalare a Kaspersky Endpoint Security.

Dacă dorești să pornești Kaspersky Endpoint Security, fă clic pe butonul **Terminare**.

Dacă dorești să închizi Expertul de configurare inițială fără a porni Kaspersky Endpoint Security, golește caseta de selectare **Pornire Kaspersky Endpoint Security 10 pentru Windows** și fă clic pe **Terminare**.

## Declarația referitoare la Kaspersky Security Network

În acest pas ești invitat să participi în Kaspersky Security Network.

Citește Declarația referitoare la Kaspersky Security Network:

- Dacă ești de acord cu toți termenii, selectează opțiunea **Accept termenii de participare la Kaspersky Security Network** în fereastra Expertului de configurare inițială.
- Dacă nu ești de acord cu termenii de participare la Kaspersky Security Network, selectează opțiunea **Nu accept termenii de participare la Kaspersky Security Network** în fereastra Expertului de configurare inițială.

Pentru a continua Expertul de configurare inițială, fă clic pe **OK**.

## Despre modalitățile de efectuare a unui upgrade pentru o versiune veche de aplicație

Pentru a face upgrade unei versiuni anterioare a aplicației la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, decriptează toate unitățile de hard disk criptate.

Poți face upgrade următoarelor aplicații la Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (versiunea 6.0.4.1424) / MP4 CF2 (versiunea 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (versiunea 6.0.4.1424) / MP4 CF2 (versiunea 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (versiunea 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (versiunea 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (versiunea 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (versiunea 10.2.5.3201).

Atunci când se efectuează upgrade pentru oricare dintre aplicațiile listate mai sus la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, conținutul directoarelor Carantină și Copie de rezervă nu este transferat.

Poți face upgrade la o versiune veche a aplicației după cum urmează:



- Local, în mod interactiv, folosind Expertul de configurare a aplicației.
- Local, în mod neinteractiv, din [linia de comandă](#)
- La distanță, folosind suita software Kaspersky Security Center (vezi *Ghidul de implementare Kaspersky Security Center*)
- La distanță, prin Editorul de politică de grup din Microsoft Windows (vezi fișierele de ajutor din sistemul de operare)

Atunci când faci upgrade unei versiuni anterioare la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, nu este nevoie să elimini versiunea anterioară a aplicației. Recomandăm închiderea tuturor aplicațiilor înainte de a efectua upgrade pentru o versiune anterioară de aplicație.

## Se elimină aplicația

Această secțiune descrie cum poți elimina Kaspersky Endpoint Security de pe computer.

## Despre modalitățile de eliminare a aplicației

Eliminarea aplicației Kaspersky Endpoint Security lasă computerul și datele utilizatorului neprotejate împotriva amenințărilor.

Aplicația Kaspersky Endpoint Security poate fi eliminată de pe computer în mai multe moduri:

- Local, în mod interactiv, folosind [Expertul Configurare](#)
- Local, în mod neinteractiv, din [linia de comandă](#)
- La distanță, folosind suita software Kaspersky Security Center (vezi *Ghidul de implementare Kaspersky Security Center* pentru detalii)
- La distanță, prin Editorul de politică de grup din Microsoft Windows (vezi fișierele de ajutor din sistemul de operare)

## Eliminarea aplicației folosind Expertul de instalare

*Pentru a elimina Kaspersky Endpoint Security folosind Expertul de instalare:*

1. În meniul **Start**, selectează **Aplicații > Kaspersky Endpoint Security 10 for Windows > Modificare, reparare sau eliminare**.

Expertul de instalare pornește.

2. În fereastra **Modificare, reparare sau eliminare aplicație** a expertului de instalare, fă clic pe butonul **Eliminare**.

3. Urmează instrucțiunile din Expertul de instalare.

## Pasul 1. Salvarea datelor aplicației pentru utilizare ulterioară

În timpul acestui pas, puteți specifica care sunt datele utilizate de aplicație pe care doriți să le păstrați pentru utilizare ulterioară la instalarea următoare a aplicației (de exemplu, la instalarea unei versiuni mai noi). Dacă nu specificați niciun fel de date, aplicația va fi complet eliminată.

*Pentru a salva datele aplicației pentru utilizare ulterioară,*

bifează casetele de selectare de lângă tipurile de date pe care dorești să le salvezi:

- **Date de activare** – date care elimină necesitatea activării aplicației pe care o veți instala în viitor. Aplicația este activată în mod automat în baza licenței curente, cât timp licența nu a expirat la momentul instalării.
- **Fișiere copiate de rezervă și în carantină** – fișiere care sunt scanate de aplicație și sunt plasate în Copie de rezervă sau în Carantină.

Fișierele din Copie de rezervă și carantină care sunt salvate după eliminarea aplicației pot fi accesate numai din aceeași versiune a aplicației care a fost folosită pentru salvarea acelor fișiere.

Dacă intenționezi folosește obiectele din Copie de rezervă și Carantină după eliminarea aplicației, trebuie să le restaurezi din locația lor de stocare înainte de a elimina aplicația. Cu toate acestea, experții Kaspersky nu recomandă restaurarea fișierelor din Copie de rezervă și Carantină, deoarece aceasta ar putea dăuna computerului.

- **Setări operaționale ale aplicației** – valori ale setărilor aplicației care sunt selectate în timpul configurării aplicației.
- **Stocare locală a cheilor de criptare** – date care oferă acces direct la fișiere și dispozitive care au fost criptate înainte de eliminarea aplicației. Fișierele și unitățile criptate pot fi accesate direct după reinstalarea aplicației cu funcționalitatea de criptare.

Această casetă de selectare este bifată în mod implicit.

Pentru a lansa Expertul de instalare, fă clic pe butonul **Următorul**. Pentru a opri Expertul de instalare, fă clic pe butonul **Revocare**.

## Pasul 2. Confirmarea eliminării aplicației

Deoarece eliminarea aplicației amenință securitatea computerului, ți se solicită confirmarea faptului că vrei să elimini aplicația. Pentru aceasta, fă clic pe butonul **Eliminare**.

Pentru a opri oricând eliminarea aplicației, poți revoca această operație făcând clic pe butonul **Revocare**.

## Pasul 3. Eliminarea aplicației. Finalizarea eliminării

În acest pas, Expertul de instalare elimină aplicarea de pe computer. Așteaptă până când eliminarea aplicației este finalizată.

Atunci când elimini aplicația, sistemul de operare poate necesita o repornire. Dacă decizi să nu repornești imediat, finalizarea procedurii de eliminare a aplicației se amână până când sistemul de operare este repornit sau până când computerul este oprit și apoi repornit.

## Eliminarea aplicației din linia de comandă

Poți porni procesul de dezinstalare a aplicației din linia de comandă. Dezinstalarea este executată în modul interactiv sau în modul silențios (fără a lansa Expertul de instalare a aplicației).

*Pentru a lansa procesul de dezinstalare a aplicației în modul interactiv,*

în linia de comandă tastează `setup.exe /x` sau `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Expertul de instalare pornește. Urmează instrucțiunile din [Expertul de instalare](#).

*Pentru a lansa procesul de dezinstalare a aplicației în modul silențios,*

în linia de comandă tastează `setup.exe /s /x` sau `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Această acțiune lansează procesul de dezinstalare a aplicației în modul silențios (fără a lansa Expertul de instalare).

Dacă operațiunea de dezinstalare a aplicației este protejată prin parolă, trebui să introduci numele de utilizator și parola corespunzătoare în linia de comandă.

*Pentru a elimina aplicația din linia de comandă în modul interactiv atunci când sunt configurate numele de utilizator și parola pentru autentificare în cazul eliminării, modificării sau reparării Kaspersky Endpoint Security:*

În linia de comandă, tastează `setup.exe /pKLLLOGIN=<Nume utilizator> /pKLASSWD=***** /x` sau

`msiexec.exe KLLLOGIN=<Nume utilizator> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Expertul de instalare pornește. Urmează instrucțiunile din [Expertul de instalare](#).

*Pentru a elimina aplicația din linia de comandă în modul silențios atunci când sunt configurate numele de utilizator și parola pentru autentificare în cazul eliminării, modificării sau reparării Kaspersky Endpoint Security:*

În linia de comandă, tastează `setup.exe /pKLLLOGIN=<Nume utilizator> /pKLASSWD=***** /s /x` sau

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLLOGIN=<Nume utilizator> KLPASSWD=***** /qn`.

## Ștergerea obiectelor și a datelor rămase după operațiunea de testare a Agentului de Autentificare

În cursul dezinstalării aplicației, dacă Kaspersky Endpoint Security detectează obiecte și date care au rămas pe unitatea de hard disk de sistem după operațiunea de testare pentru Agentul de Autentificare, dezinstalarea aplicației este întreruptă și devine imposibilă până când aceste obiecte și date nu sunt eliminate.

Obiectele și datele pot rămâne pe unitatea de hard disk de sistem după operațiunea de testare pentru Agentul de Autentificare numai în cazuri excepționale. De exemplu, acest lucru se poate întâmpla dacă computerul nu a fost repornit după aplicarea unei politici a Kaspersky Security Center cu setări de criptare sau dacă aplicația nu reușește să pornească după operațiunea de testare pentru Agentul de Autentificare.

Poți elimina obiectele și datele rămase pe unitatea de hard disk de sistem după operațiunea de testare pentru Agentul de Autentificare în două moduri:

- Folosind politica aplicației Kaspersky Security Center.
- Folosind Utilitarul Restaurare.

*Pentru a folosi o politică a aplicației Kaspersky Security Center pentru a elimina obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare:*

1. Aplică pe computer o politică a aplicației Kaspersky Security Center cu setările configurate pentru [decriptarea](#) tuturor unităților de hard disk ale computerului.
2. Pornește Kaspersky Endpoint Security.

*Pentru a folosi utilitarul Restaurare pentru a elimina obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare:*

1. Pornește Utilitarul de restaurare executând fișierul executabil fdert.exe [creat folosindu-se Kaspersky Endpoint Security](#) pe computer având conectată unitatea de hard disk de sistem pe care rămân obiectele și datele după operațiunea de testare a Agentului de Autentificare.
2. În lista verticală **Selectare dispozitiv** din fereastra utilitarului Restaurare, selectează unitatea de hard disk de sistem pe care se găsesc obiectele și datele de șters.
3. Fă clic pe butonul **Scanare**.
4. Fă clic pe butonul **Ștergere obiecte și date AA**.

Această acțiune pornește procesul de eliminare a obiectelor și datelor rămase după operațiunea de testare pentru Agentul de Autentificare.

După eliminarea obiectelor și a datelor rămase după operațiunea de testare pentru Agentul de Autentificare, este posibil să fie nevoie să elimini și informațiile despre incompatibilitatea aplicației cu Agentul de Autentificare.

*Pentru a elimina informațiile despre incompatibilitatea aplicației cu Agentul de Autentificare,*

tastează comanda `avp pbatestreset` în linia de comandă.

Componentele de criptare trebuie să fie instalate pentru a putea executa comanda `avp pbatestreset`.

## Interfața aplicației

Această secțiune descrie elementele principale ale interfeței aplicației.

## Pictograma aplicației din zona de notificare a barei de activități




Imediat după instalarea produsului Kaspersky Endpoint Security, pictograma aplicației apare în zona de notificare a barei de activități Microsoft Windows.

Pictograma are următoarele funcții:

- Indică activitatea aplicației.
- Acționează ca o comandă rapidă la meniul contextual și la fereastra principală ale aplicației.

## Indicarea activității aplicației

Pictograma aplicației are rolul de indicator al activității aplicației:

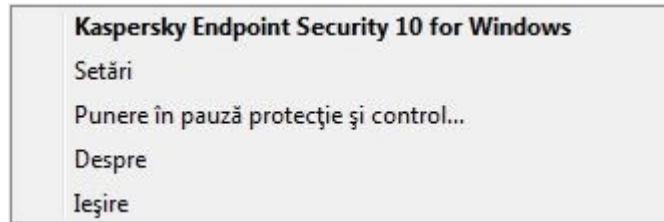
- Pictograma  semnifică faptul că toate componentele de protecție ale aplicației sunt activate.
- Pictograma  semnifică faptul că în funcționarea aplicației Kaspersky Endpoint Security au avut loc evenimente importante care necesită atenția. De exemplu, Antivirusul pentru fișiere este dezactivat sau bazele de date ale aplicației sunt neactualizate.
- Pictograma  semnifică faptul că în funcționarea aplicației Kaspersky Endpoint Security au apărut evenimente critice. De exemplu, o eroare în funcționarea unei componente sau deteriorarea bazelor de date ale aplicației.

## Meniul contextual al pictogramei aplicației

Meniul contextual al pictogramei aplicației conține următoarele elemente:

- **Kaspersky Endpoint Security 10 for Windows.** Deschide fila **Protecție și control** din fereastra principală a aplicației. Fila **Protecție și control** îți permite să reglezi funcționarea componentelor și activităților aplicației și să vizualizezi statisticile privind fișierele procesate și amenințările detectate.
- **Setări.** Deschide fila **Setări** din fereastra principală a aplicației. Fila **Setări** îți permite să modifice setările implicite ale aplicației.
- **Pauză protecție și control / Reluare protecție și control.** Trece temporar în pauză/reia funcționarea componentelor de protecție și control ale aplicației. Acest element din meniul contextual nu influențează activitatea de actualizare sau activitățile de scanare, fiind disponibil numai atunci când politica aplicației Kaspersky Security Center este dezactivată.
- **Dezactivare politică / Activare politică.** Dezactivează/activează politica aplicației Kaspersky Security Center. Acest element de meniu contextual este disponibil atunci când Kaspersky Endpoint Security funcționează în baza unei politici și a fost setată o parolă pentru dezactivarea politicii aplicației Kaspersky Security Center.

- **Despre.** Acest element deschide o fereastră informativă cu detaliile aplicației.
- **Ieșire.** Acest element determină închiderea aplicației Kaspersky Endpoint Security. Dacă faci clic pe acest element al meniului contextual, aplicația este descărcată din memoria RAM a computerului.



Meniul contextual al pictogramei aplicației








Poți deschide meniul contextual al pictogramei aplicației poziționând indicatorul mouse-ului deasupra acesteia în zona de notificare a barei de activități Microsoft Windows și făcând clic pe ea.

## Fereastra principală a aplicației

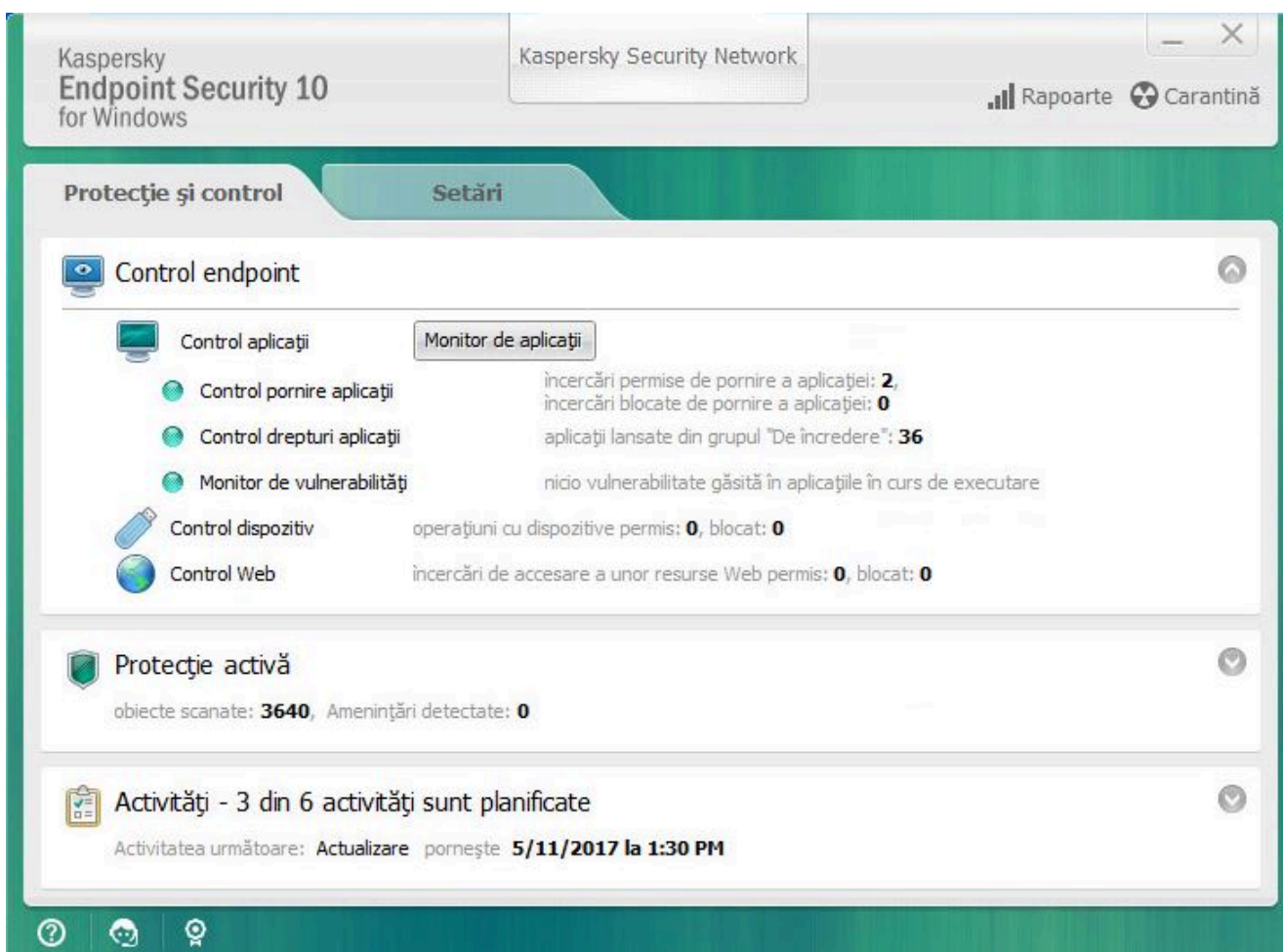
Fereastra principală a aplicației Kaspersky Endpoint Security conține elemente de interfață care asigură accesul la funcțiile principale ale aplicației.

Fereastra principală a aplicației este împărțită în patru părți (vezi imaginea de mai jos):

- Partea de sus a ferestrei conține elementele de interfață care îți permit să vizualizezi informațiile următoare:
  - Detaliile aplicației
  - Statistici Kaspersky Security Network
  - Lista de fișiere neprocesate
  - Lista de vulnerabilități detectate
  - Lista de fișiere din carantină
  - Stocarea fișierelor infectate șterse de aplicație
  - Rapoartele despre evenimentele care au apărut în timpul funcționării aplicației sau a fiecărei componente a aplicației ori în timpul efectuării unor activități
- Fila **Protecție și control** îți permite să reglezi funcționarea componentelor aplicației și finalizarea activităților. Fila **Protecție și control** este afișată atunci când deschizi fereastra principală a aplicației.
- Fila **Setări** îți permite să editezi setările implicite ale aplicației.

- Partea de jos a ferestrei principale conține următoarele elemente:
  - **Buton** . Fă clic pe acest buton pentru a fi direcționat către sistemul de ajutor al aplicației Kaspersky Endpoint Security.
  - **Buton** . Fă clic pe acest buton pentru a deschide fereastra **Asistență** care conține informații despre sistemul de operare, versiunea curentă a aplicației Kaspersky Endpoint Security și linkuri către resursele de informații Kaspersky.
  - **Buton**  / . Fă clic pe acest buton pentru a deschide fereastra **Licențiere**, care conține informații despre licența curentă.
  - **Buton**  /  / . Fă clic pe acest buton pentru a deschide fereastra **Evenimente** care conține informații despre actualizările disponibile, precum și solicitări de a accesa fișiere și dispozitive criptate.

Butonul este disponibil numai atunci când există solicitări de acces sau actualizări neinstalate.



Fereastra principală a aplicației

*Pentru a deschide fereastra principală a aplicației Kaspersky Endpoint Security, efectuează una dintre acțiunile următoare:*

- Fă clic pe pictograma aplicației în zona de notificări din bara de activități Microsoft Windows.



- Selectează **Kaspersky Endpoint Security 10 for Windows** în [meniul contextuale al pictogramei aplicației](#).

## Fila Configurare setări aplicație

Fila cu setările aplicației Kaspersky Endpoint Security îți permite să configurezi setările generale ale aplicației, componente individuale, rapoarte și spații de stocare, activități de scanare, activități de scanare pentru detectare de vulnerabilități și comunicarea cu serverele Kaspersky Security Network.

Fila cu setările aplicației este compusă din două părți (vezi figura de mai jos):

- Partea din stânga conține componentele aplicației, activitățile și o secțiune de setări avansate care include mai multe subsecțiuni.
- Partea din dreapta conține elemente de control pe care le poți folosi pentru a configura setările componente sau activității selectate în stânga ferestrei, precum și setări avansate.



Fila Configurare setări aplicație

*Pentru a deschide fila de setări ale aplicației, efectuează una dintre acțiunile următoare:*

- În [fereastra principală a aplicației](#), selectează fila **Setări**.
- În [meniul contextual al pictogramei aplicației](#), selectează **Setări**.

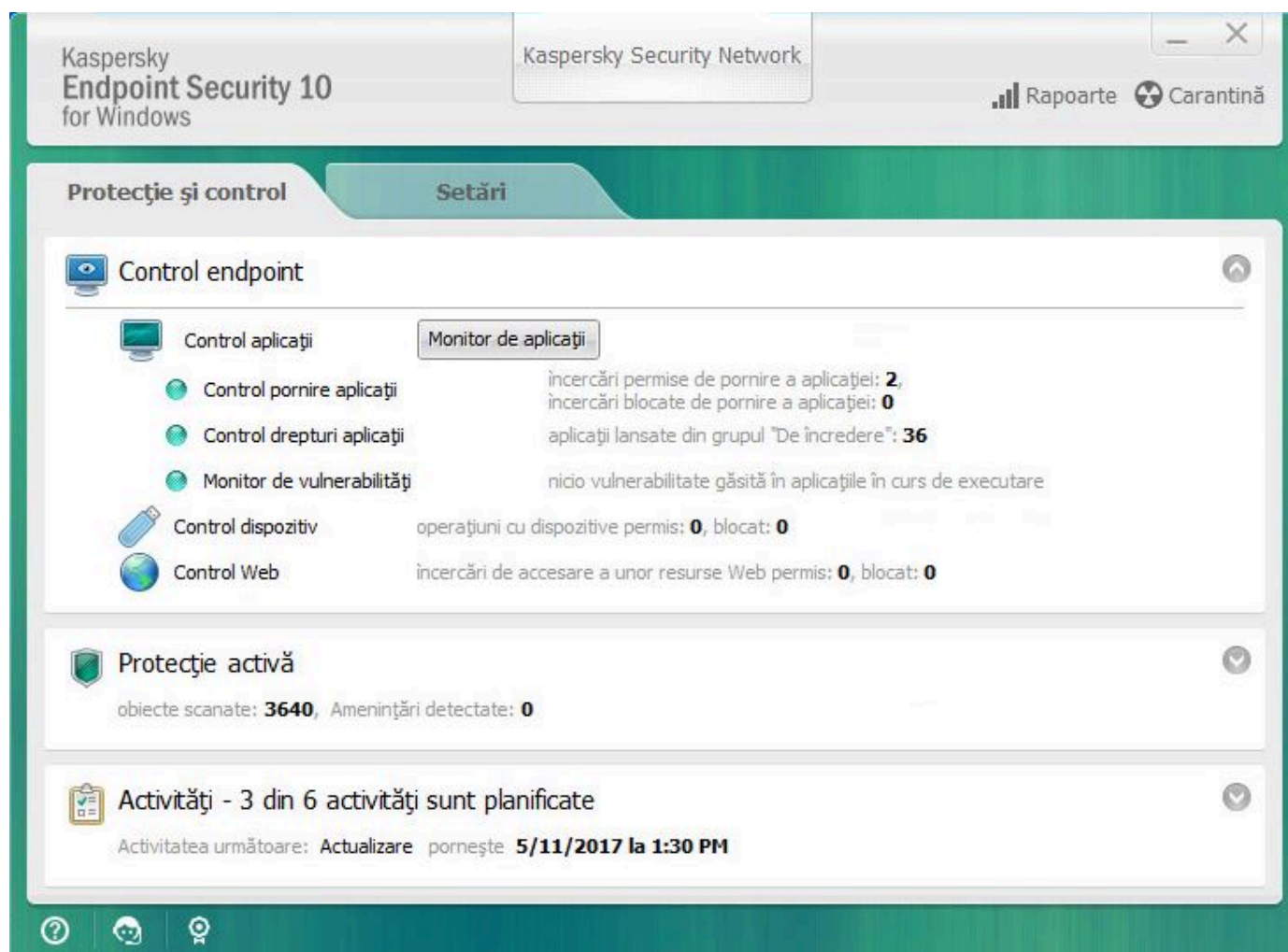
## Fila Protecție și control aplicație

Fila Protecție și control din Kaspersky Endpoint Security are menirea de a furniza informații generale despre performanțele tuturor activităților și despre funcționarea tuturor componentelor aplicației. În această filă poți și să reglezi funcționarea componentelor și performanțele activităților.

Fila Protecție și control aplicație are trei părți (vezi imaginea de mai jos):

- Secțiunea **Control endpoint** conține o listă de componente de control.
- Secțiunea **Gestionare protecție** conține o listă de componente ale protecției antivirus.
- Secțiunea **Activități** conține o listă de activități locale care sunt executate pe computer.

Fiecare secțiune conține elemente de control pe care le poți folosi pentru a activa sau a dezactiva funcționarea unei componente, pentru a accesa setările componentei sau activității selectate și pentru a vedea statistici privind funcționarea componentei sau activității selectate.



Fila Protecție și control aplicație

*Pentru a deschide fila Protecție și control aplicație, executa una dintre acțiunile următoare:*

- În [fereastra principală a aplicației](#), selectează fila **Protecție și control**.
- Fă clic pe pictograma aplicației în zona de notificări din bara de activități Microsoft Windows.
- Selectează **Kaspersky Endpoint Security 10 for Windows** în [meniul contextuale al pictogramei aplicației](#).

## Licența aplicației

Această secțiune furnizează informații despre conceptele generale legate de licențierea aplicației.

## Despre Acordul de licență pentru utilizatorul final

*Acordul de licență pentru utilizatorul final* este un acord obligatoriu între tine și AO Kaspersky Lab, care stipulează condițiile în care poți folosi aplicația.

Recomandăm citirea cu atenție a termenilor din Acordul de licență pentru utilizatorul final înainte de utilizarea aplicației.

Poți vedea termenii din Acordul de licență în următoarele moduri:

- La instalarea aplicației Kaspersky Endpoint Security în [modul interactiv](#).
- Citind fișierul license.txt. Acest document este inclus în [kitul de distribuire al aplicației](#).

Confirmând acceptarea Acordului de licență pentru utilizatorul final, indici acceptare termenilor Acordului de licență pentru utilizatorul final. Dacă nu accepți termenii din Acordul de licență pentru utilizatorul final, trebuie să abandonezi instalarea.

## Despre licență

O *licență* este un drept pe durată limitată de utilizare a aplicației acordat în baza Acordului de licență pentru utilizatorul final.

O licență validă îți dă dreptul la următoarele tipuri de servicii:

- Utilizarea aplicației în conformitate cu termenii Acordului de licență pentru utilizatorul final
- Asistență tehnică

Scopul serviciilor și perioada de utilizare a aplicației depind de tipul de licență cu care a fost activată aplicația.


Există două tipuri de licență:

- *Trial* – o licență gratuită destinată încercării aplicației.

O licență trial are, de obicei, un termen scurt. După expirarea licenței trial, toate caracteristicile aplicației Kaspersky Endpoint Security sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie să achiziționezi o licență comercială.

Puteți activa aplicația sub licență pentru versiune trial o singură dată.

- *Comercială* – o licență plătită furnizată atunci când achiziționezi Kaspersky Endpoint Security.

Funcționalitatea aplicației disponibilă în baza licenței comerciale depinde de alegerea produsului. Produsul selectat este indicat în [Certificat licență](#). Informații despre produsele disponibile pot fi găsite pe [site-ul web Kaspersky](#) .

Atunci când expiră licența comercială, caracteristicile principale ale aplicației sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie să reînnoiești licența comercială. Dacă nu intenționezi să îți reînnoiești licența, trebuie să elimini aplicația de pe computer.

## Despre certificatul de licență

Un *certificat de licență* este un document transferat utilizatorului împreună cu un fișier cheie sau un cod de activare.

Certificatul de licență conține următoarele informații despre licență:

- Numărul comenzii
- Detalii despre utilizatorul căruia îi este acordată licența
- Detalii despre aplicația care poate fi activată utilizându-se licența
- Limitarea privind numărul de unități licențiate (de exemplu, numărul de dispozitive pe care poate fi utilizată aplicația în baza licenței)
- Data de început a termenului licenței
- Data de expirare a licenței sau termenul licenței
- Tipul de licență

## Despre abonament

*Abonamentul pentru Kaspersky Endpoint Security* este o comandă de achiziție pentru aplicație, cu anumiți parametri (dată de expirare a abonamentului, număr de dispozitive protejate). Poți comanda un abonament pentru Kaspersky Endpoint Security de la furnizorul tău de servicii (de exemplu, un ISP). Un abonament poate fi reînnoit manual sau automat și poate fi anulat. Îți poți administra abonamentul pe [site-ul Web al furnizorului de servicii](#).

Abonamentul poate fi limitat (pentru un an de zile, de exemplu) sau nelimitat (fără o dată de expirare). Pentru ca aplicația Kaspersky Endpoint Security să funcționeze după expirarea termenului unui abonament limitat, trebuie să-ți reînnoiești abonamentul. Abonamentul nelimitat este reînnoit automat dacă serviciile furnizorului au fost plătite anticipat în timp util.

În cazul unui abonament limitat, la expirarea sa, ți se va oferi o perioadă de grație pentru reînnoirea abonamentului, perioadă în care aplicația își va păstra funcționalitatea. Furnizorul de servicii va decide dacă ți se va acorda sau nu o perioadă de grație și, dacă da, va stabili și durata perioadei de grație.

Pentru a folosi Kaspersky Endpoint Security în baza unui abonament, trebuie să aplici codul de activare primit de la furnizorul de servicii. După aplicarea codului de activare, cheia activă este instalată. Cheia activă definește licența pentru utilizarea aplicației în baza abonamentului. O cheie suplimentară poate fi instalată numai folosind un cod de activare și nu poate fi instalată folosind un fișier cheie sau în baza unui abonament.

Funcționalitatea aplicației disponibilă în baza abonamentului poate corespunde funcționalității aplicației pentru următoarele tipuri de licențe pentru versiune comercială: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Licențele de acest tip sunt destinate protejării serverelor de fișiere, stațiilor de lucru și dispozitivelor mobile și suportă utilizarea componentelor de control pe stații de lucru și dispozitive mobile.

Opțiunile de administrare a abonamentului posibile pot diferi de la un furnizor de servicii la altul. Furnizorul de servicii este posibil să nu ofere o perioadă de grație pentru reînnoirea abonamentului, în care aplicația să își păstreze funcționalitatea.

Codurile de activare achiziționate în baza unui abonament nu pot fi folosite pentru a activa versiuni anterioare ale Kaspersky Endpoint Security.

## Despre codul de activare

Un *cod de activare* este o succesiune unică de caractere alfanumerice, compusă din douăzeci de cifre și litere din alfabetul latin, pe care o primești atunci când achiziționezi o licență pentru versiune comercială pentru Kaspersky Endpoint Security.

Pentru a activa aplicația folosind un cod de activare, este necesar acces la Internet pentru conectarea la serverele de activare Kaspersky.

Atunci când aplicația este activată folosind un cod de activare, este instalată cheia activă. O cheie suplimentară poate fi instalată numai folosind un cod de activare și nu poate fi instalată folosind un fișier cheie sau în baza unui abonament.

Dacă se pierde un cod de activare după activarea aplicației, îl poți restaura. Este posibil să ai nevoie de un cod de activare, de exemplu, pentru a înregistra un cont Kaspersky CompanyAccount. Pentru a restaura un cod de activare, trebuie să [contactezi Asistența tehnică de la Kaspersky](#).

## Despre cheie

O *cheie* este o secvență alfanumerică unică. O cheie face posibilă utilizarea aplicației în baza termenilor indicați în Certificatul de licență (tip de licență, perioadă de valabilitate a licenței, restricții ale licenței).

Un certificat de licență nu este furnizat pentru o cheie instalată în baza unui abonament.

O cheie poate fi adăugată la aplicație folosind un cod de activare sau un fișier cheie.

Poți adăuga, edita sau șterge chei. Cheia poate fi blocată de către Kaspersky dacă au fost încălcați termenii din Acordul de licență pentru utilizatorul final. Dacă o cheie este introdusă în lista neagră, trebuie să adaugi o altă cheie pentru a continua să folosești aplicația.

Dacă a fost ștearsă o cheie pentru o licență expirată, funcționalitatea aplicației nu este disponibilă. Nu poți adăuga din nou o astfel de cheie după ce a fost ștearsă.

Există două tipuri de chei: active și suplimentare.

O *cheie activă* este o cheie care este utilizată în mod curent de aplicație. O cheie trial sau o cheie pentru licență pentru versiune comercială poate fi adăugată drept cheie activă. Aplicația nu poate avea mai mult de o singură cheie activă.

O *cheie suplimentară* este o cheie care dă dreptul utilizatorului să folosească aplicația, dar care nu este în prezent în uz. La expirarea cheii active, o cheie suplimentară devine activă în mod automat. O cheie suplimentară poate fi adăugată numai dacă este disponibilă o cheie activă.

O cheie pentru o licență trial poate fi adăugată numai drept cheie activă. Ea nu poate fi adăugată drept cheie suplimentară. O cheie pentru licență trial nu poate înlocui cheia activă pentru o licență pentru versiune comercială.

Dacă o cheie este introdusă în lista neagră, funcționalitatea aplicației definită de [licența în baza căreia a fost activată aplicația](#) rămâne disponibilă timp de opt zile. Kaspersky Security Network și actualizările pentru baza de date și pentru modulele aplicației sunt disponibile fără restricții. Aplicația îl notifică pe utilizator că această cheie a fost introdusă în lista neagră. După opt zile, funcționalitatea aplicației va fi limitată la nivelul de funcționalitate disponibil după expirarea termenului licenței: aplicația operează fără actualizări și Kaspersky Security Network nu este disponibil.

## Despre fișierul cheie

Un *fișier cheie* este un fișier cu extensia .key pe care-l primești de la Kaspersky după achiziționarea Kaspersky Endpoint Security. Scopul unui fișier cheie este acela de a adăuga o cheie care activează aplicația.

Nu trebuie să te conectezi la serverele de activare Kaspersky pentru a activa aplicația cu un fișier cheie.

Poți recupera un fișier cheie dacă acesta a fost șters în mod accidental. Vei avea nevoie de un fișier cheie pentru a înregistra un cont Kaspersky CompanyAccount, de exemplu.

Pentru a recupera un fișier cheie, procedează într-unul din modurile următoare:

- Contactați vânzătorul licenței.
- Obține un fișier cheie de pe [site-ul Web Kaspersky](#), pe baza codului de activare existent.

Atunci când aplicația este activată folosind un fișier cheie, este adăugată o cheie activă. O cheie de licență de rezervă poate fi adăugată numai folosind un fișier cheie și nu poate fi adăugată folosind un cod de activare.

## Despre furnizarea datelor


Acceptând Acordului de licență pentru utilizatorul final, ești de acord să transferi în mod automat informații cu privire la utilizarea de către tine a produsului, precum și tipul, versiunea și localizarea lingvistică a programului instalat, identificatorul unic al programului de instalare a programului și tipul de instalare și date despre chei active și suplimentare (inclusiv tipul de licență, perioada de valabilitate, data activării programului și data expirării licenței, numărul licenței, starea actuală a licenței, versiunea protocolului de interacțiune cu serverul de activare).



În cazul în care programul este activat cu un cod de activare, pentru a primi informații statistice privind distribuția și utilizarea produselor Titularului licenței, ești de acord să furnizezi în mod automat versiunea a programului utilizat (inclusiv informații despre actualizările de program instalate, identificatorul de instalare a programului, precum și informații privind licențele), versiunea sistemului de operare și identificatorii componentelor programului activi în momentul furnizării informațiilor.



Informațiile primite sunt protejate de Kaspersky conform legii și cerințelor și regulamentelor aplicabile ale Kaspersky.

Kaspersky folosește informațiile primite absolut anonim și numai sub formă de date statistice generale. Statisticile generale sunt generate automat utilizând informațiile colectate inițial și nu conțin niciun fel de date personale sau orice alt tip de informații confidențiale. Informațiile colectate inițial sunt distruse și acumulate (o dată pe an). Datele statistice generale sunt stocate pe termen nedefinit.

Citește Acordul de licență pentru utilizatorul final și vizitează [site-ul Web Kaspersky](#)  pentru a afla mai multe despre cum colectăm, procesăm, depozităm și distrugem informații despre utilizarea aplicației după ce accepți Acordul de licență pentru utilizatorul final și ești de acord cu Declarația KSN. Fișierele license.txt și ksn.txt files conțin Acordul de licență pentru utilizatorul final și Declarația KSN și fac parte din [pachetul de distribuție](#) pentru program.

## Vizualizarea informațiilor despre licență

*Pentru a vizualiza informațiile despre licență:*



1. Deschide [fereastra principală a aplicației](#).
2. Fă clic pe butonul  /  în partea de jos a ferestrei principale a aplicației.

Se va deschide fereastra **Licențiere**. Informațiile despre licență sunt afișate în secțiunea din partea de sus a ferestrei **Licențiere**.

## Achiziționarea unei licențe

Poți achiziționa o licență după instalarea aplicației. După achiziționarea unei licențe, vei primi un cod de activare sau un fișier cheie pentru [activarea aplicației](#).

*Pentru a achiziționa o licență:*

1. Deschide [fereastra principală a aplicației](#).
2. Fă clic pe butonul  /  în partea de jos a ferestrei principale a aplicației.

Se va deschide fereastra **Licențiere**.

3. În fereastra **Licențiere**, efectuează una dintre următoarele acțiuni:



- Dacă nu au fost adăugate chei sau a fost adăugată o cheie pentru o licență pentru versiune trial, fă clic pe butonul **Achiziționare licență**.
- Dacă este adăugată cheia pentru o licență pentru versiune comercială, fă clic pe butonul **Reînnoiește licența**.

Se va deschide o fereastră cu magazinul online Kaspersky, unde poți achiziționa o licență.

## Reînnoirea unei licențe

Atunci când licența se apropie de expirare, o poți reînnoi. Astfel computerul tău rămâne protejat după expirarea licenței existente și până când activezi aplicația cu o nouă licență.

*Pentru a reînnoi o licență:*

1. [Primește](#) un cod de activare a aplicației nou sau un fișier cheie nou.
2. [Adaugă o cheie suplimentară](#) cu codul de activare sau fișierul cheie pe care l-ai primit.

O [cheie suplimentară ?](#) este adăugată drept rezultat. Ea devine [activă ?](#) la expirarea licenței.

Poate dura ceva timp până când cheia este actualizată de la cheie suplimentară la cheie activă, din cauza distribuirii încărcării între serverele de activare ale Kaspersky.

## Reînnoirea abonamentului

Atunci când folosești aplicația în baza unui abonament, Kaspersky Endpoint Security contactează în mod automat serverul de activare la intervale specificate, până când abonamentul tău expiră.

Dacă folosești aplicația în baza unui abonament nelimitat, Kaspersky Endpoint Security verifică în fundal serverul de activare pentru a găsi eventuale chei reînnoite. Dacă pe serverul de activare este disponibilă o cheie, aplicația o adaugă, înlocuind cheia anterioară. Astfel, abonamentul nelimitat pentru Kaspersky Endpoint Security este reînnoit fără implicarea utilizatorului.



Dacă folosești aplicația în baza unui abonament limitat, în ziua în care abonamentul expiră (sau în care perioada de grație de după abonament expiră, în cursul căreia reînnoirea abonamentului este disponibilă), Kaspersky Endpoint Security prezintă o notificare corespunzătoare și oprește încercarea de a reînnoi abonamentul automat. În acest caz, Kaspersky Endpoint Security se comportă la fel ca atunci când [expiră o licență pentru versiune comercială pentru aplicație](#): aplicația operează fără actualizări, iar Kaspersky Security Network nu este disponibil.

Îți poți reînnoi abonamentul [pe site-ul Web al furnizorului de servicii](#).

Îți poți reînnoi manual abonamentul în fereastra **Licențiere**. Acest lucru poate fi necesar dacă abonamentul a fost reînnoit după expirarea perioadei de grație și aplicația nu a actualizat automat starea abonamentului.

## Vizitarea site-ului Web al furnizorului de servicii

*Pentru a vizita site-ul Web al furnizorului de servicii din interfața aplicației:*

1. Deschide [fereastra principală a aplicației](#).
2. Fă clic pe butonul  /  în partea de jos a ferestrei principale a aplicației.  
Se va deschide fereastra **Licențiere**.
3. În fereastra **Licențiere**, fă clic pe **Contactează furnizorul abonamentului tău**.

## Despre metoda de activare a aplicației

*Activarea* este procesul de activare a unei licențe care îți permite să folosești o versiune complet funcțională a aplicației, până când licența expiră. Procesul de activare a aplicației implică adăugarea unei chei.

Poți activa aplicația folosind unul din următoarele moduri:

- Atunci când instalezi aplicația, cu ajutorul [Expertului de configurare inițială](#). În acest mod poți adăuga cheia activă.
- Local, din interfața aplicației, folosind [Expertul de activare](#). În acest mod poți adăuga atât cheia activă, cât și o cheie suplimentară.
- La distanță, cu suita software Kaspersky Security Center, [creând](#) și apoi [pornind](#) o activitate de adăugare cheie. În acest mod poți adăuga atât cheia activă, cât și o cheie suplimentară.
- La distanță, distribuind chei și coduri de activare stocate în zona de stocare a cheilor de pe serverul de administrare Kaspersky Security Center către computere client (vezi *Ghidul de administrare Kaspersky Security Center* pentru detalii). În acest mod poți adăuga atât cheia activă, cât și o cheie suplimentară.

Codul de activare achiziționat în baza abonamentului este distribuit primul.

- Folosind [linia de comandă](#).

Poate dura ceva timp până când aplicația este activată folosind un cod de activare (indiferent că este vorba despre o instalare la distanță sau neinteractivă), din cauza distribuirii încărcării între serverele de activare ale Kaspersky. Dacă trebuie să activezi aplicația imediat, poți întrerupe procesul de activare în curs și poți începe activarea folosind Expertul de activare.

## Utilizarea Expertului de activare pentru activarea aplicației

*Pentru a activa Kaspersky Endpoint Security folosind Expertul de activare:*

1. Fă clic pe butonul  /  în partea de jos a ferestrei principale a aplicației.

Se va deschide fereastra **Licențiere**.

2. În fereastra **Licențiere**, fă clic pe butonul **Activare aplicație cu licență nouă**.

Expertul de activare a aplicației pornește.

3. Urmează instrucțiunile din Expertul de activare.

Pentru informații mai detaliate despre procedura de activare a aplicației, consultă secțiunea [Expertul de configurare inițială](#).

## Activarea aplicației din linia de comandă

*Pentru a activa aplicația din linia de comandă,*

tastează `avp.com license /add <cod activare sau fișier licență> /password=<parolă>` în linia de comandă.

## Pornirea și oprirea aplicației

Această secțiune descrie modul de configurare a pornirii automate a aplicației, de pornire sau oprire manuală a aplicației și de trecere în pauză sau de reluare a funcționării componentelor de protecție și control.

## Activarea și dezactivarea pornirii automate a aplicației

Dacă pornirea automată este activată, aplicația Kaspersky Endpoint Security pornește imediat după ce pornește sistemul de operare, fără intervenția utilizatorului. Această opțiune de pornire a aplicației este activată în mod implicit.

După instalare, Kaspersky Endpoint Security pornește automat pentru prima dată. Ulterior, aplicația pornește automat după ce pornește sistemul de operare.

Descărcarea bazelor de date antivirus ale Kaspersky Endpoint Security după pornirea sistemului de operare poate dura până la două minute, în funcție de computer. În acest interval, nivelul de protecție a computerului este redus. Descărcarea bazelor de date antivirus atunci când Kaspersky Endpoint Security este pornit pe un sistem de operare deja încărcat nu cauzează o reducere a nivelului de protecție a computerului.

*Pentru a activa sau a dezactiva pornirea automată a aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Protecție antivirus** din stânga.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi rularea automată a aplicației, bifează caseta de selectare **Pornire Kaspersky Endpoint Security 10 for Windows la pornirea computerului**.
  - Dacă dorești să dezactivezi rularea automată a aplicației, debifează caseta de selectare **Pornire Kaspersky Endpoint Security 10 for Windows la pornirea computerului**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Pornirea și oprirea manuală a aplicației

Experții Kaspersky nu recomandă oprirea manuală a aplicației Kaspersky Endpoint Security, deoarece astfel computerul și datele personale sunt expuse la amenințări. Dacă este necesar, poți [trece în pauză protecția computerului](#) atât timp cât este necesar, fără a opri aplicația.

Aplicația Kaspersky Endpoint Security trebuie pornită manual dacă anterior ai dezactivat [pornirea automată a aplicației](#).

*Pentru a porni manual aplicația:*

În meniul **Start**, selectează **Aplicații Kaspersky Endpoint Security 10 for Windows**.



*Pentru a opri manual aplicația:*

1. Fă clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În meniul contextual, selectează **leșire**.

## Trecerea în pauză și reluarea protecției și controlului computerului

Trecerea în pauză a protecției și controlului computerului înseamnă dezactivarea tuturor componentelor de protecție și control ale aplicației Kaspersky Endpoint Security pentru un timp.

Starea aplicației este afișată folosind [pictograma aplicației în zona de notificări din bara de activități](#).

- Pictograma  indică faptul că protecția și controlul computerului au fost trecute în pauză.
- Pictograma  indică faptul că protecția și controlul computerului au fost dezactivate.

Trecerea în pauză sau reluarea protecției și controlului computerului nu afectează activitățile de scanare sau de actualizare.

Dacă, atunci când treci în pauză sau reiei protecția și controlul computerului, sunt deja stabilite conexiuni la rețea, se afișează o notificare despre terminarea acestor conexiuni.

*Pentru a trece în pauză protecția și controlul computerului:*

1. Fă clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În meniul contextual, selectează **Trecere în pauză protecție și control**.  
Se deschide fereastra **Pauză protecție**.
3. Selectează una dintre următoarele opțiuni:

- **Pauză pentru timpul specificat** – Protecția și controlul computerului se reiau după intervalul de timp specificat în lista verticală de mai jos.
- **Pauză până la repornire** – Protecția și controlul computerului se reiau după ce închizi și deschizi din nou aplicația ori repornești sistemul de operare. Pornirea automată a aplicației trebuie să fie activată pentru a folosi această opțiune.
- **Pauză** – Protecția și controlul computerului se reiau atunci când decizi să le reiei.

4. Dacă la pasul precedent ai selectat opțiunea **Pauză pentru timpul specificat**, selectează intervalul necesar în lista verticală.

*Pentru a relua protecția și controlul computerului:*

1. Fă clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În meniul contextual, selectează **Reluare protecție și control**.

Poți relua oricând protecția și controlul computerului, indiferent care este opțiunea de trecere în pauză a protecției și a controlului computerului selectată anterior.

## Protejarea sistemului de fișiere al computerului. Antivirus pentru fișiere

Această secțiune conține informații despre Antivirusul pentru fișiere și instrucțiuni despre cum se configurează setările acestei componente.

### Despre Antivirusul pentru fișiere

Antivirusul pentru fișiere împiedică infectarea sistemului de fișiere al computerului. În mod implicit, Antivirusul pentru fișiere pornește odată cu aplicația Kaspersky Endpoint Security, rămâne permanent activ în memoria computerului și scanează toate fișierele deschise, salvate sau lansate pe computer și pe toate unitățile atașate la acesta, pentru a detecta prezența virușilor și altor amenințări.

La detectarea unei amenințări într-un fișier, Kaspersky Endpoint Security execută următoarele acțiuni:

1. Identifică tipul de obiect detectat în fișier (cum ar fi un *virus* sau un *troian*).
2. Etichetează fișierul drept *probabil infectat*, dacă scanarea nu poate determina dacă fișierul este sau nu infectat. Este posibil ca fișierul să conțină o secvență de cod tipică pentru viruși sau alte programe malware sau un cod modificat al unui virus cunoscut.
3. Aplicația afișează o [notificare](#) despre obiectul periculos detectat în fișier (dacă sunt configurate notificările) și procesează fișierul luând [acțiunea](#) specificată în setările Antivirusului pentru fișiere.





### Activarea și dezactivarea Antivirusului pentru fișiere

Antivirusul pentru fișiere este activat în mod implicit, rulând în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva Antivirusul pentru fișiere.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva Antivirusul pentru fișiere din fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Protecție**.  
Se deschide secțiunea **Protecție**.
4. Fă clic dreapta pentru a accesa meniul contextual al liniei cu informații despre componenta Antivirus pentru fișiere.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa Antivirusul pentru fișiere, selectează **Pornire** în meniu.  
Pictograma de stare a componentei, , care se afișează în stânga liniei **Antivirus pentru fișiere**, se transformă în pictograma .
  - Pentru a dezactiva Antivirusul pentru fișiere, selectează **Opre** în meniu.  
Pictograma de stare a componentei, , care se afișează în stânga liniei **Antivirus pentru fișiere**, se transformă în pictograma .

*Pentru a activa sau a dezactiva Antivirusul pentru fișiere din fereastra cu setările aplicației:*

1. Deschide fereastra cu setările aplicației.
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi Antivirusul pentru fișiere, bifează caseta de selectare **Activare Antivirus pentru fișiere**.
  - Dacă dorești să dezactivezi Antivirusul pentru fișiere, debifează caseta de selectare **Activare Antivirus pentru fișiere**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Trecerea automată în pauză a Antivirusului pentru fișiere

Poți configura componenta Antivirus pentru fișiere astfel încât să treacă automat în pauză la o oră specificată sau atunci când utilizezi anumite programe.

Trecerea în pauză a componentei Antivirus pentru fișiere atunci când aceasta generează conflicte cu anumite programe reprezintă o măsură de urgență. În cazul apariției oricărui conflict în timpul funcționării unei componente, recomandăm contactarea Serviciului de asistență tehnică al Kaspersky (<https://companyaccount.kaspersky.com>). Specialiștii serviciului de asistență te vor ajuta să configurezi componenta Antivirus pentru fișiere astfel încât aceasta să se execute simultan cu alte programe de pe computer.

*Pentru a configura trecerea automată în pauză a Antivirusului pentru fișiere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru fișiere**.
4. În fereastra **Antivirus pentru fișiere**, selectează fila **Suplimentar**.
5. În secțiunea **Pauză activitate**:
  - Pentru a configura trecerea automată în pauză a Antivirusului pentru fișiere la o anumită oră, bifează caseta de selectare **După planificare** și fă clic pe butonul **Planificare**.  
Se deschide fereastra **Pauză activitate**.
  - Pentru a configura trecerea automată în pauză a Antivirusului pentru fișiere la pornirea anumitor aplicații, bifează caseta de selectare **La pornirea aplicației** și fă clic pe butonul **Selectare**.  
Se deschide fereastra **Aplicații**.
6. Efectuează una dintre următoarele acțiuni:
  - În cazul în care configurezi trecerea automată în pauză a Antivirusului pentru fișiere la o oră specificată, în fereastra **Pauză activitate**, utilizează câmpurile **Pauză activitate la** și **Reluare activitate la** pentru a specifica perioada (în format OO:MM) în decursul căreia Antivirusul pentru fișiere trebuie trecut în pauză. Fă clic pe **OK**.



- În cazul în care configurezi trecerea automată în pauză a Antivirusului pentru fișiere la pornirea aplicațiilor specificate, utilizează butoanele **Adăugare**, **Editare** și **Eliminare** din fereastra **Aplicații** pentru a crea o listă de aplicații în cursul funcționării cărora Antivirusul pentru fișiere trebuie trecut în pauză. Fă clic pe **OK**.

7. În fereastra **Antivirus pentru fișiere**, fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea Antivirusului pentru fișiere

Pentru a configura Antivirusul pentru fișiere, poți efectua următoarele acțiuni:

- Schimbă nivelul de securitate.

Poți să selectezi unul dintre nivelurile de securitate presetate sau să configurezi manual setările pentru nivelul de securitate. Dacă modifizi setările pentru nivelul de securitate, poți reveni oricând la setările recomandate pentru nivelul de securitate.

- Schimbă acțiunea efectuată de Antivirusul pentru fișiere la detectarea unui fișier infectat.

- Editează domeniului de protecție al Antivirusului pentru fișiere.

Poți extinde sau restrânge domeniul de protecție adăugând sau eliminând obiectele de scanat sau schimbând tipurile de fișiere de scanat.

- Configurează analizorul euristic.

Antivirusul pentru fișiere utilizează o tehnică denumită analiză a semnăturii. La analiza semnăturii, Antivirusul pentru fișiere compară obiectul detectat cu înregistrările din bazele de date antivirus ale aplicației. În urma recomandărilor experților Kaspersky, analiza semnăturii este activată în permanență.

Pentru a spori eficiența protecției, poți utiliza analiza euristică. În timpul analizei euristice, Antivirusul pentru fișiere analizează activitatea obiectelor în sistemul de operare. Analiza euristică activează detectarea de obiecte periculoase pentru care momentan nu este disponibilă nicio înregistrare în baza de date antivirus a aplicației.

- Optimizează scanarea.

Poți optimiza scanarea de fișiere efectuată de Antivirusul pentru fișiere, reducând astfel durata de scanare și mărinv viteza de funcționare a aplicației Kaspersky Endpoint Security. Acest lucru se obține prin scanarea numai a fișierelor noi și a celor care au fost modificate din momentul scanării ulterioare. Acest mod se aplică atât fișierelor simple, cât și celor compuse.

De asemenea, poți activa utilizarea tehnologiilor iChecker și iSwift, care optimizează viteza de scanare a fișierelor excluzând fișierele care nu au fost modificate din momentul celei mai recente scanări.

- Configurează scanarea fișierelor compuse.
- Schimbă modul de scanare a fișierelor.

## Schimbarea nivelului de securitate

Pentru a proteja sistemul de fișiere al computerului, Antivirusul pentru fișiere aplică diverse grupuri de setări. Aceste grupuri de setări sunt denumite *niveluri de securitate*. Sunt preinstalate trei niveluri de securitate presetate: **Ridicat**, **Recomandat** și **Redus**. Setările pentru nivelul de securitate **Recomandat** sunt considerate a fi setările optime recomandate de către experții de la Kaspersky.

*Pentru a modifica un nivel de securitate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. În secțiunea **Nivel de securitate**, efectuează una dintre următoarele acțiuni:
  - Dacă dorești să setezi unul dintre nivelurile de securitate presetate (**Ridicat**, **Recomandat** sau **Redus**), selectează-l folosind cursorul.
  - Dacă dorești să configurezi un nivel particularizat de securitate, fă clic pe butonul **Setări** și introdu setările tale particularizate în fereastra **Antivirus pentru fișiere** care se deschide.  
După ce configurezi un nivel particularizat de securitate, numele nivelului de securitate din secțiunea **Nivel de securitate** devine **Particularizat**.
  - Dacă dorești ca nivelul de securitate să devină cel **Recomandat**, fă clic pe butonul **Implicit**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Schimbarea acțiunii efectuate de Antivirusul pentru fișiere asupra fișierelor infectate

*Pentru a schimba acțiunea efectuată de Antivirusul pentru fișiere asupra fișierelor infectate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.

3. În secțiunea **Acțiune la detectarea amenințării**, selectează opțiunea necesară:


- **Selectare automată acțiune.**
- **Efectuare acțiune: Dezinfectare. Șterge dacă nu se reușește dezinfectarea.**
- **Efectuare acțiune: Dezinfectare.**

Chiar dacă această opțiune este selectată, Kaspersky Endpoint Security aplică acțiunea **Eliminare** fișierelor care fac parte din aplicația Windows Store.

- **Efectuare acțiune: Eliminare.**
- **Efectuare acțiune: Blocare.**

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Editarea domeniului de protecție al Antivirusului pentru fișiere

Domeniul de protecție desemnează obiectele pe care componenta le scanează atunci când este activată. Proprietățile domeniilor de protecție diferă de la o componentă la alta. Locațiile și tipurile de fișiere care urmează a fi scanate reprezintă proprietățile domeniului de protecție al Antivirusului pentru fișiere. În mod implicit, Antivirusul pentru fișiere scanează numai fișierele infectate  care sunt stocate pe hard diskuri, unități de rețea sau medii amovibile.

*Pentru a crea domeniul de protecție:*

1. Deschide fereastra cu setările aplicației.
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru fișiere**.
4. În fereastra **Antivirus pentru fișiere**, selectează fila **General**.
5. În secțiunea **Tipuri de fișiere**, specifică tipurile de fișiere pe care dorești să le scaneze componenta Antivirus pentru fișiere:
  - Dacă dorești să scanezi toate fișierele, selectează **Toate fișierele**.

- Dacă dorești să scanezi fișierele ale căror formate sunt cele mai vulnerabile la infectare, selectează **Fișiere scanate după format**.
- Dacă dorești să scanezi fișierele ale căror extensii sunt cele mai vulnerabile la infectare, selectează **Fișiere scanate după extensie**.

Când selectezi tipurile de fișiere de scanat, reține următoarele informații:

- Există unele formate de fișiere (precum .txt) pentru care probabilitatea de pătrundere a codului rău intenționat și de activare ulterioară a acestuia este destul de redusă. În același timp, există formate de fișiere care conțin sau pot conține cod executabil (precum .exe, .dll și .doc). Riscul de pătrundere și de activare a codului rău intenționat în astfel de fișiere este destul de ridicat.
- Un intrus poate trimite pe computerul tău un virus sau alt program rău intenționat într-un fișier executabil care a fost redenumit cu extensia .txt. Dacă selectezi scanarea fișierelor după extensie, un astfel de fișier este omis de scanare. Dacă se selectează scanarea fișierelor după format, atunci Antivirusul pentru fișiere analizează antetul fișierelor indiferent de extensia acestora. Această analiză poate dezvălui faptul că formatul fișierului este .exe. Un astfel de fișier este scanat complet în vederea detectării de viruși și alte programe rău intenționate.

6. În secțiunea **Domeniu de protecție**, efectuează una dintre următoarele acțiuni:

- Dacă dorești să adaugi un obiect nou la domeniul de scanare, fă clic pe butonul **Adăugare**.
- Dacă dorești să schimbi locația unui obiect, selectează obiectul în domeniul de scanare și fă clic pe butonul **Editare**.

Se deschide fereastra **Selectare domeniu de scanare**.

- Dacă dorești să elimini un obiect din lista de obiecte de scanat, selectează-l și fă clic pe butonul **Eliminare**.

Se deschide o fereastră pentru confirmarea ștergerii.

7. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să adaugi un obiect nou sau să schimbi locația unui obiect din lista de obiecte de scanat, selectează obiectul în fereastra **Selectare domeniu de scanare** și fă clic pe butonul **Adăugare**.

Toate obiectele selectate în fereastra **Selectare domeniu de scanare** sunt afișate în fereastra **Antivirus pentru fișiere**, în lista **Domeniu de protecție**.

Fă clic pe **OK**.

- Dacă dorești să elimini un obiect, fă clic pe butonul **Da** în fereastra pentru confirmarea eliminării.

8. Dacă este necesar, repetă pașii 6-7 pentru a adăuga, a muta sau a elimina obiecte din lista de obiecte de scanat.
9. Pentru a exclude un obiect din lista de obiecte de scanat, debifează caseta de selectare de lângă obiect din lista **Domeniu de protecție**. Totuși, obiectul rămâne în lista de obiecte de scanat, cu toate că este exclus de la scanarea efectuată de Antivirusul pentru fișiere.
10. În fereastra **Antivirus pentru fișiere**, fă clic pe **OK**.
11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Utilizarea analizorului euristic cu Antivirusul pentru fișiere

*Pentru a configura utilizarea analizorului euristic la funcționarea Antivirusului pentru fișiere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru fișiere**.
4. În fereastra **Antivirus pentru fișiere**, selectează fila **Performanță**.
5. În secțiunea **Metode de scanare**:
  - Dacă dorești ca Antivirusul pentru fișiere să utilizeze analiza euristică, bifează caseta de selectare **Analiză euristică** și utilizează cursorul pentru a seta nivelul analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.
  - Dacă nu dorești ca Antivirusul pentru fișiere să utilizeze analiza euristică, debifează caseta de selectare **Analiză euristică**.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Utilizarea tehnologiilor de scanare la funcționarea Antivirusului pentru fișiere

*Pentru a configura utilizarea tehnologiilor de scanare la funcționarea Antivirusului pentru fișiere:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru fișiere**.

4. În fereastra **Antivirus pentru fișiere**, selectează fila **Suplimentar**.

5. În secțiunea **Tehnologii de scanare**:

- Bifează casetele de selectare de lângă numele de tehnologii pe care dorești să le utilizezi la funcționarea Antivirusului pentru fișiere.
- Debifează casetele de selectare de lângă numele de tehnologii pe care nu dorești să le utilizezi la funcționarea Antivirusului pentru fișiere.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Optimizarea scanării de fișiere

*Pentru a optimiza scanarea de fișiere:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.

3. Fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru fișiere**.

4. În fereastra **Antivirus pentru fișiere**, selectează fila **Performanță**.

5. În secțiunea **Optimizare scanare**, bifează caseta de selectare **Scanare numai fișiere noi și modificate**.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Scanarea fișierelor compuse

O tehnică obișnuită pentru ascunderea virușilor și a altor programe malware o reprezintă introducerea încorporarea acestora în fișiere compuse, precum arhive sau baze de date. Pentru a detecta virușii și celelalte programe malware ascunse în acest mod, fișierul compus trebuie dezarhivat, fapt care poate încetini scanarea. Poți limita setul de fișiere compuse de scanat, accelerând astfel scanarea.

Metoda folosită pentru procesarea unui fișier compus infectat (dezinfectare sau ștergere) depinde de tipul de fișier.

Componenta Antivirus pentru fișiere dezinfectează fișiere compuse în formatele RAR, ARJ, ZIP, CAB și LHA și șterge fișiere în toate celelalte formate (exceptând bazele de date de e-mail).

*Pentru a configura scanarea fișierelor compuse:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru fișiere**.
4. În fereastra **Antivirus pentru fișiere**, selectează fila **Performanță**.
5. În secțiunea **Scanare fișiere compuse**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de instalare sau fișiere în formate Office.
6. Pentru a scana doar fișierele compuse noi și modificate, bifează caseta de selectare **Scanare numai fișiere noi și modificate**.  
Antivirus pentru fișiere va scana numai fișierele compuse noi și modificate de toate tipurile.
7. Fă clic pe butonul **Suplimentar**.  
Se deschide fereastra **Fișiere compuse**.

8. În secțiunea **Scanare în fundal**, efectuează una dintre următoarele acțiuni:

- Pentru a împiedica Antivirusul pentru fișiere să dezarhiveze în fundal fișierele compuse, debifează caseta de selectare **Dezarhivare fișiere compuse în fundal**.
- Pentru a permite ca Antivirusul pentru fișiere să dezarhiveze fișierele compuse atunci când scanează în fundal, bifează caseta de selectare **Dezarhivare fișiere compuse în fundal** și specifică valoarea necesară în câmpul **Dimensiune minimă fișier**.

9. În secțiunea **Limită dimensiune**, efectuează una dintre următoarele acțiuni:

- Pentru a bloca Antivirusul pentru fișiere să dezarhiveze fișierele compuse de dimensiuni mari, bifează caseta de selectare **Nu dezarhiva fișiere compuse mari** și specifică valoarea necesară în câmpul **Dimensiune maximă fișier**. Antivirusul pentru fișiere nu va dezarhiva fișierele compuse mai mari decât dimensiunea specificată.

- Pentru a permite ca Antivirusul pentru fișiere să dezarhiveze fișierele compuse de dimensiuni mari, debifează caseta de selectare **Nu dezarhiva fișiere compuse mari**.

Un fișier este considerat mare dacă dimensiunea sa depășește valoarea din câmpul **Dimensiune maximă fișier**.

Antivirusul pentru fișiere scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este sau nu bifată caseta de selectare **Nu dezarhiva fișiere compuse mari**.

10. Fă clic pe **OK**.

11. În fereastra **Antivirus pentru fișiere**, fă clic pe **OK**.

12. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Schimbarea modului de scanare

*Modul de scanare* reprezintă starea în care Antivirusul pentru fișiere pornește scanarea de fișiere. În mod implicit, Kaspersky Endpoint Security scanează fișierele în modul inteligent. În acest mod de scanare a fișierelor, Antivirusul pentru fișiere decide dacă scanează sau nu fișierele în urma operațiunilor de analiză a fișierelor efectuate de utilizator, de o aplicație desemnată de utilizator (din contul utilizat pentru Log in sau dintr-un alt cont de utilizator) sau de sistemul de operare. De exemplu, atunci când se lucrează cu un document Microsoft Office Word, Kaspersky Endpoint Security scanează fișierul la prima deschidere și la ultima închidere a acestuia. Operațiunile intermediare care suprascriu fișierul nu determină scanarea acestuia.

*Pentru a schimba modul de scanare a fișierelor:*

1. Deschide [fereastra cu setările aplicației](https://support.kaspersky.com/KESWin/10SP2/ro-RO/all-in-one.htm).



2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru fișiere**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru fișiere.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru fișiere**.

4. În fereastra **Antivirus pentru fișiere**, selectează fila **Suplimentar**.

5. În secțiunea **Mod de scanare**, selectează modul necesar:

- **Mod inteligent.**
- **La accesare și modificare.**
- **La accesare.**
- **La executare.**

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Protecția pentru e-mail. Antivirus pentru e-mail

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre Antivirusul pentru e-mail și instrucțiuni despre cum se configurează setările acestei componente.

## Despre Antivirusul pentru e-mail

Antivirusul pentru e-mail scanează mesajele de e-mail primite și trimise în vederea detectării de viruși și alte amenințări. Acesta pornește odată cu aplicația Kaspersky Endpoint Security, rămâne permanent activ în memoria computerului și scanează toate mesajele trimise sau primite prin protocoalele POP3, SMTP, IMAP, MAPI și NNTP. Dacă în mesaj nu este detectată nicio amenințare, mesajul devine disponibil și/sau este procesat.

Dacă în mesajul de e-mail este detectată o amenințare, Antivirusul pentru e-mail efectuează următoarele acțiuni:


1. Identifică tipul de obiect detectat în mesajul de e-mail (de exemplu, *troian*).

2. Unul mesaj de e-mail i se atribuie una dintre următoarele stări:

- *Probabil infectat*. Această stare este atribuită dacă scanarea nu poate determina dacă mesajul de e-mail este sau nu infectat cu siguranță. Este posibil ca mesajul de e-mail să conțină o secțiune de cod care este tipică pentru viruși sau alte programe malware sau un cod modificat al unui virus cunoscut.
- *Infectat*. Această stare este atribuită unui obiect dacă scanarea unui mesaj de e-mail găsește o secțiune de cod a unui virus cunoscut care este inclus în bazele de date antivirus ale Kaspersky Endpoint Security.
- *Negăsit*. Această stare este atribuită unui obiect dacă scanarea unui mesaj de e-mail nu detectează viruși sau alte amenințări.

Apoi aplicația blochează mesajul de e-mail, afișează o [notificare](#) despre obiectul detectat (dacă se specifică astfel în setările de notificare) și efectuează acțiunea care este specificată în setările componentei Antivirus pentru e-mail.

Această componentă interacționează cu clienții de e-mail instalați pe computer. Este disponibilă o extensie încorporabilă pentru clientul de e-mail Microsoft Office Outlook, care permite ajustarea setărilor de scanare a mesajelor. Extensia Antivirus pentru e-mail este încorporată în clientul de e-mail Microsoft Office Outlook în cursul instalării aplicației Kaspersky Endpoint Security.

Funcționarea Antivirus pentru e-mail este ilustrată de pictograma aplicației, care este afișată în zona de notificări din bara de activități. Atunci când Antivirus pentru e-mail scanează un mesaj de e-mail, pictograma aplicației se schimbă la .

## Activarea și dezactivarea Antivirusului pentru e-mail

Antivirusul pentru e-mail este activat în mod implicit, executându-se în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva Antivirusul pentru e-mail.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva Antivirusul pentru e-mail din fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.

2. Selectează fila **Protecție și control**.

### 3. Fă clic pe secțiunea **Protecție**.



Se deschide secțiunea **Protecție**.

### 4. Fă clic dreapta pentru a accesa meniul contextual al liniei cu informații despre componenta Antivirus pentru e-mail.



Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.

### 5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa Antivirusul pentru e-mail, selectează **Pornire** în meniu.

Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus pentru e-mail**, se transformă în pictograma .

- Pentru a dezactiva Antivirusul pentru e-mail, selectează **Oprire** în meniu.

Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus pentru e-mail**, se transformă în pictograma .

*Pentru a activa sau a dezactiva Antivirusul pentru e-mail din fereastra cu setările aplicației:*

#### 1. Deschide fereastra cu setările aplicației.

#### 2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.

#### 3. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să activezi Antivirusul pentru e-mail, bifează caseta de selectare **Activare Antivirus pentru e-mail**.
- Dacă dorești să dezactivezi Antivirusul pentru e-mail, debifează caseta de selectare **Activare Antivirus pentru e-mail**.

#### 4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea Antivirusului pentru e-mail

Pentru a configura Antivirusul pentru e-mail, poți efectua următoarele acțiuni:

- Schimbă nivelul de securitate pentru e-mail.

Poți selecta unul dintre nivelurile preinstalate de securitate a e-mailului sau poți configura un nivel particularizat de securitate a e-mailului.

Dacă ai modificat setările pentru nivelul de securitate a e-mailului, poți reveni oricând la setările recomandate pentru nivelul de securitate a e-mailului.

- Schimbă acțiunea pe care Kaspersky Endpoint Security o efectuează asupra mesajelor infectate.
- Editează domeniului de protecție al Antivirusului pentru e-mail.

- Configurează scanarea fișierelor compuse atașate la mesaje de e-mail.

Poți activa sau dezactiva scanarea atașărilor la mesaje de e-mail, poți limita dimensiunea maximă a atașărilor la mesaje de scanat și poți limita durata maximă de scanare a unei atașări la un mesaj.

- Configurează filtrarea atașărilor la mesaje de e-mail în funcție de tipul acestora.

Filtrarea atașărilor la mesaje în funcție de tip permite redenumirea sau ștergerea automată a fișierelor ale căror tipuri sunt specificate.

- Configurează analizorul euristic.

Pentru a spori eficiența protecției, poți utiliza [analiza euristică ?](#). În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea aplicațiilor în sistemul de operare. Analiza euristică poate detecta în mesaje amenințări pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

- Configurează scanarea e-mailurilor în Microsoft Office Outlook.

Este disponibilă o extensie încorporabilă pentru clientul de e-mail Microsoft Office Outlook, pentru permite configurarea convenabilă a setărilor pentru scanarea mesajelor.

Dacă lucrezi cu alți clienți de e-mail, inclusiv Microsoft Outlook Express, Windows Mail și Mozilla Thunderbird, componenta Antivirus pentru e-mail scanează traficul trimis prin protocoalele SMTP, POP3, IMAP și NNTP.

Dacă lucrezi cu clientul de e-mail Mozilla Thunderbird, componenta Antivirus pentru e-mail nu scanează de viruși și alte programe rău intenționate mesajele transmise prin protocolul IMAP, dacă sunt utilizate filtre pentru mutarea mesajelor din directorul **Inbox**.

## Schimbarea nivelului de securitate a e-mailului

Antivirusul pentru e-mail aplică diverse grupuri de setări pentru a proteja e-mailul. Grupurile de setări sunt denumite *niveluri de securitate a e-mailului*. Sunt preinstalate trei niveluri de securitate a e-mailului: **Ridicat**, **Recomandat** și **Redus**. Nivelul **Recomandat** de securitate a e-mailului este considerat setarea optimă și este recomandat de Kaspersky.

*Pentru a schimba nivelului de securitate a e-mailului:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.
3. În secțiunea **Nivel de securitate**, efectuează una dintre următoarele acțiuni:
  - Dacă dorești să utilizezi unul dintre nivelurile preinstalate de securitate a e-mailului (**Ridicat**, **Recomandat** sau **Redus**), utilizează cursorul pentru a selecta un nivel.
  - Dacă dorești să configurezi un nivel particularizat de securitate a e-mailului, fă clic pe butonul **Setări** și specifică setările în fereastra **Antivirus pentru e-mail**.  
După ce configurezi un nivel particularizat de securitate a e-mailului, numele nivelului de securitate din secțiunea **Nivel de securitate** devine **Particularizat**.
  - Dacă dorești ca nivelul de securitate a e-mailului să devină cel **Recomandat**, fă clic pe butonul **Implicit**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Schimbarea acțiunii de efectuat asupra mesajelor de e-mail infectate

*Pentru a schimba acțiunea de efectuat asupra mesajelor de e-mail infectate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.
3. În secțiunea **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze atunci când este detectat un mesaj infectat:
  - **Selectare automată acțiune.**
  - **Efectuare acțiune: Dezinfectare. Șterge dacă nu se reușește dezinfectarea.**
  - **Efectuare acțiune: Dezinfectare.**
  - **Efectuare acțiune: Eliminare.**
  - **Efectuare acțiune: Blocare.**

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Editarea domeniului de protecție al Antivirusului pentru e-mail

Domeniul de protecție se referă la obiectele care sunt scanate de către componentă atunci când este activă. Proprietățile domeniilor de protecție diferă de la o componentă la alta. Proprietățile domeniului de protecție al Antivirusului pentru e-mail includ setările de integrare a Antivirusului pentru e-mail în clienți de e-mail și tipurile de mesaje de e-mail și de protocoale de e-mail al căror trafic este scanat de Antivirusul pentru e-mail. În mod implicit, aplicația Kaspersky Endpoint Security scanează atât mesajele de e-mail primite, cât și pe cele trimise, precum și traficul efectuat prin protocoalele POP3, SMTP, NNTP și IMAP și este integrată în clientul de e-mail Microsoft Office Outlook.

*Pentru a crea domeniul de protecție al Antivirusului pentru e-mail:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.

3. Fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru e-mail**.

4. Selectează fila **General**.

5. În secțiunea **Domeniu de protecție**, efectuează una dintre următoarele acțiuni:

- Dacă dorești ca Antivirusul pentru e-mail să scaneze toate mesajele primite și trimise pe/de pe computer, selectează opțiunea **Mesaje primite și trimise**.
- Dacă dorești ca Antivirusul pentru e-mail să scaneze numai mesajele primite pe computer, selectează opțiunea **Numai mesaje primite**.

Dacă alegi să scanezi numai mesajele primite, se recomandă să efectuezi o scanare pentru toate mesajele trimise, deoarece există posibilitatea ca pe computerul tău să existe viermi de e-mail care se răspândesc prin e-mail. Acest lucru contribuie la evitarea problemelor rezultate din trimiterea nemonitorizată de mesaje e-mail infectate de pe computerul tău.

6. În secțiunea **Conectivitate**, efectuează următoarele acțiuni:

- Dacă dorești ca Antivirusul pentru e-mail să scaneze mesajele transmise prin protocoalele POP3, SMTP, NNTP și IMAP înainte de a ajunge pe computerul tău, bifează caseta de selectare **Trafic POP3/SMTP/NNTP/IMAP**.

Dacă nu dorești ca Antivirusul pentru e-mail să scaneze mesajele transmise prin protocoalele POP3, SMTP, NNTP și IMAP înainte de a ajunge pe computerul tău, debifează caseta de selectare **Trafic POP3/SMTP/NNTP/IMAP**. În acest caz, mesajele sunt scanate de către extensia Antivirus pentru e-mail încorporată în clientul de e-mail Microsoft Office Outlook după ce sunt primite pe computerul utilizatorului, dacă este bifată caseta de selectare **Suplimentar: extensie Microsoft Office Outlook**.

Dacă utilizezi un alt client de e-mail decât Microsoft Office Outlook, mesajele de e-mail transmise prin protocoalele POP3, SMTP, NNTP și IMAP nu sunt scanate de către componenta Antivirus pentru e-mail atunci când caseta de selectare **Trafic POP3/SMTP/NNTP/IMAP** nu este bifată.

- Dacă dorești să asiguri accesul la setările Antivirusului pentru fișiere din Microsoft Office Outlook și să permiți ca mesajele transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI să fie scanate după ce ajung pe computer folosind extensia încorporată în Microsoft Office Outlook, bifează caseta de selectare **Suplimentar: extensie Microsoft Office Outlook**.

Dacă dorești să blochezi accesul la setările Antivirusului pentru fișiere din Microsoft Office Outlook și să dezactivezi scanarea mesajelor transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI după ce ajung pe computer folosind extensia încorporată în Microsoft Office Outlook, debifează caseta de selectare **Suplimentar: extensie Microsoft Office Outlook**.

Extensia Antivirus pentru e-mail este încorporată în clientul de e-mail Microsoft Office Outlook în cursul instalării aplicației Kaspersky Endpoint Security.

7. Fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Scanarea fișierelor compuse atașate la mesaje de e-mail

*Pentru a configura scanarea fișierelor compuse care sunt atașate la mesaje de e-mail:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.

3. Fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru e-mail**.

4. Selectează fila **General**.

5. Execută următoarea acțiune în secțiunea **Scanare fișiere compuse**:

- Dacă dorești ca Antivirusul pentru e-mail să ignore arhivele atașate la mesaje, debifează caseta de selectare **Scanare arhive atașate**.
- Dacă dorești ca Antivirusul pentru e-mail să ignore atașările de mesaje a căror dimensiune este mai mare de N megaocteți, bifează caseta de selectare **Nu scana arhive mai mari de N MO**. Dacă bifezi această casetă de selectare, specifică dimensiunea maximă a arhivei în câmpul de lângă numele casetei de selectare.
- Dacă dorești ca Antivirusul pentru e-mail să scaneze atașările de mesaje a căror scanare durează mai mult de N secunde, debifează caseta de selectare **Nu scana arhive mai multe de N s**.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Filtrarea atașărilor la mesaje de e-mail


Programele rău intenționate pot fi distribuite sub forma unor atașări în mesaje de e-mail. Poți configura filtrarea pe baza tipului de atașări la mesaje, astfel încât fișierele de tipul specificat să fie redenumite sau șterse în mod automat. Redenumind o atașare de un anumit tip, Kaspersky Endpoint Security îți poate proteja computerul împotriva executării automate a unui program rău intenționat.

*Pentru a configura filtrarea atașărilor:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru e-mail**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru e-mail.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru e-mail**.
4. În fereastra **Antivirus pentru e-mail**, selectează fila **Filtrare atașare**.



## 5. Efectuează una dintre următoarele acțiuni:

- Dacă nu dorești ca Antivirusul pentru e-mail să filtreze atașările mesajelor, selectează opțiunea **Dezactivare filtrare**.
- Dacă dorești ca Antivirusul pentru e-mail să redenumască atașările mesajelor cu [tipurile specificate](#) , selectează setarea **Redenumire tipuri de atașări specificate**.

Reține că este posibil ca formatul real al unui fișier să nu corespundă cu extensia de nume a acestuia.

Dacă activezi filtrarea de obiecte atașate la mesaje de e-mail, Antivirusul pentru e-mail poate să redenumască sau să șteargă fișiere cu următoarele extensii:

com – fișier executabil pentru o aplicație cu o dimensiune de maxim 64 KB

exe – fișier executabil sau arhivă cu dezarhivare automată

sys – fișier de sistem Microsoft Windows

prg – text de program pentru dBase, Clipper sau Microsoft Visual FoxPro sau pentru un program din suita WAVmaker

bin – fișier binar

bat – fișier de comenzi

cmd – fișier de comenzi pentru Microsoft Windows NT (similar unui fișier de comenzi pentru DOS), OS/2

dpl – bibliotecă Borland Delphi comprimată

dll – fișier bibliotecă cu legături dinamice

scr – ecran de pornire Microsoft Windows

cpl – modul panou de control Microsoft Windows

ocx – obiect Microsoft OLE (Object Linking and Embedding - Control legare și îmbinare obiect)

tsp – program care se execută în mod secvențial

drv – driver de dispozitiv

vxd – driver de dispozitiv virtual Microsoft Windows

pif – fișier de informații despre programe

lnk – fișier de link Microsoft Windows

reg – fișier cheie de registru de sistem Microsoft Windows

ini – fișier de configurare care conține date de configurare pentru Microsoft Windows, Windows NT și unele aplicații

cla – clasă Java

vbs – script Visual Basic

vbe – extensie video BIOS

js, jse – text sursă JavaScript

htm – document hipertext

htt – antet hipertext Microsoft Windows

hta – program hipertext pentru Microsoft Internet Explorer

asp – script Active Server Pages

chm – fișier HTML compilat

pht – fișier HTML cu scripturi PHP integrate

php – script integrat în fișiere HTML

wsh – fișier Microsoft Windows Script Host

wsf – script Microsoft Windows

the – fișier de tapet de fundal pentru desktop Microsoft Windows 95

hlp – fișier Ajutor Windows

eml – mesaj Microsoft Outlook Express

nws – mesaj de e-mail nou Microsoft Outlook Express

msg – mesaj de e-mail Microsoft Mail

plg – mesaj de e-mail

mbx – extensie pentru e-mailurile Microsoft Office Outlook salvate

doc\* – documente Microsoft Office Word, cum ar fi doc pentru documente Microsoft Office Word, docx pentru documente Microsoft Office Word 2007 cu suport XML și docm pentru documente Microsoft Office Word 2007 cu suport pentru macrocomenzi

dot\* – șabloane pentru documente Microsoft Office Word, cum ar fi: dot pentru șabloane de documente Microsoft Office Word, dotx pentru șabloane de documente Microsoft Office Word 2007, dotm pentru șabloane de documente Microsoft Office Word 2007 cu suport pentru macrocomenzi

fpm – program de baze de date, fișier de pornire Microsoft Visual FoxPro

rtf – document Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – bază de date de desene AutoCAD

msi – pachet Microsoft Windows Installer

otm – proiect VBA pentru Microsoft Office Outlook

pdf – document Adobe Acrobat

swf – obiect pachet Shockwave Flash

jpg, jpeg – format de elemente grafice comprimate

emf – fișier de format Metafișier extins. Următoarea generație a metafișierelor de sistem de operare Microsoft Windows. Fișierele EMF nu sunt acceptate de către sistemele de operare Microsoft Windows pe 16 biți.

ico – fișier pictogramă obiect

ov? – fișiere executabile Microsoft Office Word

xl\* – documente și fișiere Microsoft Office Excel, cum ar fi: xla, extensia pentru Microsoft Office Excel, xlc pentru diagrame, xlt pentru șabloane de documente, xlsx pentru registre de lucru Microsoft Office Excel 2007, xltm pentru registre de lucru Microsoft Office Excel 2007 cu suport pentru macrocomenzi, xlsb pentru registre de lucru Microsoft Office Excel 2007 în format binar (exceptând XML), xltx pentru șabloane Microsoft Office Excel 2007, xlsx pentru șabloane Microsoft Office Excel 2007 cu suport pentru macrocomenzi și xlam pentru plug-inuri Microsoft Office Excel 2007 cu suport pentru macrocomenzi

pp\* – documente și fișierele Microsoft Office PowerPoint, cum ar fi: pps pentru diapozitive Microsoft Office PowerPoint, ppt pentru prezentări, pptx pentru prezentări Microsoft Office PowerPoint 2007, pptm pentru prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, potx pentru șabloane de prezentări Microsoft Office PowerPoint 2007, potm pentru șabloane de prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, ppsx pentru prezentări de diapozitive Microsoft Office PowerPoint 2007, ppsm pentru prezentări de diapozitive Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi și ppam pentru plug-inuri Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi

md\* – documente și fișierele Microsoft Office Access, cum ar fi: mda pentru grupurile de lucru Microsoft Office Access și mdb pentru bazele de date

sldx – un diapozitiv Microsoft PowerPoint 2007

sldm – un diapozitiv Microsoft PowerPoint 2007 cu suport pentru macrocomenzi

thmx – o temă Microsoft Office 2007

- Dacă dorești ca Antivirusul pentru e-mail să șteargă atașările mesajelor cu tipurile specificate, selectează opțiunea **Ștergere tipuri de atașări specificate**.

6. Dacă ai selectat opțiunea **Redenumire tipuri de atașări specificate** sau opțiunea **Ștergere tipuri de atașări specificate** în cursul etapei anterioare, bifează casetele de selectare de lângă tipurile de fișiere relevante.

Poți modifica lista de tipuri de fișiere utilizând butoanele **Adăugare**, **Editare** și **Eliminare**.

7. Fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Scanarea e-mailurilor în Microsoft Office Outlook

În cursul instalării Kaspersky Endpoint Security, extensia Antivirus pentru e-mail este încorporată în Microsoft Office Outlook (denumit în continuare Outlook). Acesta permite deschiderea setărilor componentei Antivirus pentru e-mail din Outlook și specificarea momentului în care mesajele de e-mail trebuie scanate de viruși și alte amenințări. Extensia Antivirus pentru e-mail pentru Outlook poate scana mesaje primite și trimise transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI.

Setările Antivirus pentru e-mail pot fi configurate direct în Outlook dacă este bifată caseta de selectare **Suplimentar: extensie Microsoft Office Outlook** în interfața Kaspersky Endpoint Security.

În Outlook, mesajele primite sunt întâi scanate de componenta Antivirus pentru e-mail (când este bifată caseta de selectare **Trafic POP3/SMTP/NNTP/IMAP** în interfața Kaspersky Endpoint Security) și apoi de extensia Antivirus pentru e-mail pentru Outlook. În cazul în care componenta Antivirus pentru e-mail detectează un obiect periculos într-un mesaj de e-mail, te alertează despre acest eveniment.

Acțiunea pe care o alegi în fereastra de notificare determină componenta care va elimina amenințarea din mesaj: componenta Antivirus pentru e-mail sau extensia Antivirus pentru e-mail pentru Outlook.

- Dacă selectezi **Dezinfectare** sau **Eliminare** în fereastra de notificare, eliminarea amenințării va fi efectuată de componenta Antivirus pentru e-mail.
- Dacă selectezi **Omitere** în fereastra de notificare a utilizatorului, extensia Antivirus pentru e-mail pentru Outlook este cea care va elimina amenințarea.

Mesajele trimise sunt scanate mai întâi de extensia Antivirus pentru e-mail pentru Outlook și apoi de componenta Antivirus pentru e-mail.

## Configurarea scanării e-mailului în Outlook

*Pentru a configura scanarea e-mailului în Outlook 2007:*

1. Deschide fereastra principală a Outlook 2007.
2. Selectează **Service (Serviciu)** → **Settings (Setări)** din bara de meniu.  
Se deschide fereastra **Options (Opțiuni)**.
3. În fereastra **Options (Opțiuni)**, selectează fila **Email protection (Protecție e-mail)**.

*Pentru a configura scanarea e-mailului în Outlook 2010/2013:*

1. Deschide fereastra principală a Outlook.

Selectează fila **File (Fișier)** în colțul stânga-sus.

2. Fă clic pe butonul **Ascundere (Opțiuni)**.

Se deschide fereastra **Options Outlook (Opțiuni Outlook)**.

3. Selectează secțiunea **Add-Ins (Programe de completare)**.

Setările plug-inurilor încorporate în Outlook sunt afișate în partea din dreapta ferestrei.

4. Fă clic pe butonul **Add-In Options (Opțiuni program de completare)**.

## Configurarea scanării mesajelor de e-mail folosind Kaspersky Security Center

Dacă mesajele de e-mail sunt scanate folosind extensia Antivirus pentru e-mail pentru Outlook, se recomandă folosirea modului Exchange în cache. Pentru informații mai detaliate despre modul Exchange în cache și recomandări privind utilizarea sa, consultă Baza de cunoștințe Microsoft: <https://technet.microsoft.com/en-us/library/cc179175.aspx> .

*Pentru a configura modul de funcționare al extensiei Antivirus pentru e-mail pentru Outlook folosind Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi scanarea mesajelor de e-mail.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Protecție antivirus**, selectează sub-secțiunea **Antivirus pentru e-mail**.
7. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide fereastra **Antivirus pentru e-mail**.

8. În secțiunea **Conectivitate**, fă clic pe butonul **Setări**.

Se deschide fereastra **Protecție e-mail**.

9. În fereastra **Protecție e-mail**:

- Bifează caseta de selectare **Scanare la primire** dacă dorești ca extensia Antivirus pentru e-mail pentru Outlook să scaneze mesajele primite atunci când acestea ajung în mailbox.
- Bifează caseta de selectare **Scanare la citire** dacă dorești ca extensia Antivirus pentru e-mail pentru Outlook să scaneze mesajele primite atunci când utilizatorul le deschide.
- Bifează caseta de selectare **Scanare la trimitere** dacă dorești ca extensia Antivirus pentru e-mail pentru Outlook să scaneze mesajele trimise atunci când acestea sunt expediate.

10. În fereastra **Protecție e-mail**, fă clic pe **OK**.

11. În fereastra **Antivirus pentru e-mail**, fă clic pe **OK**.

12. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

## Protecția computerului pe Internet. Antivirus pentru Web

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre Antivirusul pentru Web și instrucțiuni despre cum se configurează setările acestei componente.

## Despre Antivirusul pentru Web

Ori de câte ori treci online, expui informațiile stocate pe computerul tău la viruși și alte programe malware. Acestea se pot infiltra în computer în timp ce utilizatorul descarcă software-uri gratuite sau navighezi pe site-uri Web care sunt compromise în urma atacurilor inițiate de infractori. Viermii de rețea pot găsi o cale de pătrundere pe computer imediat după ce stabilești o conexiune la Internet, chiar înainte de a deschide o pagină Web sau de a descărca un fișier.

Antivirusul pentru Web protejează datele primite și trimise pe și de pe computerul tău prin protocoalele HTTP și FTP și verifică adresele URL în raport cu lista de adrese Web periculoase sau de phishing.

Antivirusul pentru Web interceptează și analizează existența virușilor și a altor amenințări din orice pagină Web sau fișier accesat de utilizator sau de o aplicație prin intermediul protocolului HTTP sau FTP. În continuare survine una din situațiile următoare:

- Dacă se consideră că pagina sau fișierul nu conține cod rău intenționat, utilizatorul obține acces imediat la acestea.
- Dacă un utilizator accesează o pagină Web sau un fișier care conține cod periculos, aplicația efectuează acțiunea specificată în setările componentei Antivirus pentru Web.

## Activarea și dezactivarea Antivirusului pentru Web

Antivirusul pentru Web este activat în mod implicit, executându-se în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva Antivirusul pentru Web.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva Antivirusul pentru Web din fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.

2. Selectează fila **Protecție și control**.

3. Fă clic pe secțiunea **Protecție**.



Se deschide secțiunea **Protecție**.

4. Fă clic dreapta pentru a accesa meniul contextual al liniei cu informații despre componenta Antivirus pentru Web.



Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.

5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa Antivirusul pentru Web, selectează **Pornire** în meniu.

Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus pentru Web**, se transformă în pictograma .

- Pentru a dezactiva Antivirusul pentru Web, selectează **Oprește** în meniu.

Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus pentru Web**, se transformă în pictograma .



*Pentru a activa sau a dezactiva Antivirusul pentru Web din fereastra cu setările aplicației:*

1. Deschide fereastra cu setările aplicației.
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi Antivirusul pentru Web, bifează caseta de selectare **Activare Antivirus pentru Web**.
  - Dacă dorești să dezactivezi Antivirusul pentru Web, debifează caseta de selectare **Activare Antivirus pentru Web**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea Antivirusului pentru Web

Pentru a configura Antivirusul pentru Web, poți efectua următoarele acțiuni:

- Schimbă nivelul de securitate a traficului Web.  
Poți selecta unul dintre nivelurile preinstalate de securitate a traficului Web primit sau transmis prin protocoalele HTTP și FTP sau poți configura un nivel particularizat de securitate a traficului Web.  
Dacă modifizi setările pentru nivelul de securitate a traficului Web, poți reveni oricând la setările recomandate pentru nivelul de securitate a traficului Web.
- Schimbă acțiunea pe care Kaspersky Endpoint Security o efectuează asupra obiectelor de trafic Web periculoase.  
Dacă în urma analizei unui obiect HTTP se constată că acesta conține cod rău intenționat, modul în care reacționează Antivirusul pentru Web depinde de acțiunea pe care ai specificat-o.
- Configurează scanarea cu Antivirusul pentru Web a adreselor URL în bazele de date cu adrese Web periculoase.
- Configurează utilizarea analizei euristice la scanarea traficului Web pentru detectarea virușilor și altor programe rău intenționate.  
Pentru a spori eficiența protecției, poți utiliza analiza euristică. În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea aplicațiilor în sistemul de operare. Analiza euristică poate detecta amenințări pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

- Configurează utilizarea analizei euristice la scanarea paginilor Web în vederea detectării de linkuri de phishing.
- Optimizează scanarea de către Antivirusul pentru Web a traficului Web trimis și primit prin protocoalele HTTP și FTP.
- Creează o listă de adrese URL de încredere.

Poți crea o listă de adrese URL în al căror conținut ai încredere. Antivirusul pentru Web nu analizează existența virușilor și a altor amenințări în informațiile provenite de la adresele URL de încredere. Această opțiune poate fi utilă, de exemplu, atunci când Antivirusul pentru Web interferează cu descărcarea unui fișier de pe un site Web cunoscut.

O adresă URL poate fi adresa unei anumite pagini Web sau adresa unui site Web.

## Schimbarea nivelului de securitate a traficului Web

Pentru a proteja datele primite și transmise prin protocoalele HTTP și FTP, Antivirusul pentru Web aplică diverse grupuri de setări. Aceste grupuri de setări sunt denumite *niveluri de securitate a traficului Web*. Sunt preinstalate trei niveluri de securitate a traficului Web: **Ridicat**, **Recomandat** și **Redus**. Nivelul **Recomandat** de securitate a traficului Web este considerat setarea optimă și este recomandat de Kaspersky.

*Pentru a schimba nivelul de securitate a traficului Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.

În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.

3. În secțiunea **Nivel de securitate**, efectuează una dintre următoarele acțiuni:

- Dacă dorești să utilizezi unul dintre nivelurile preinstalate de securitate a traficului Web (**Ridicat**, **Recomandat** sau **Redus**), utilizează cursorul pentru a selecta un nivel.
- Dacă dorești să configurezi un nivel particularizat de securitate a traficului Web, fă clic pe butonul **Setări** și specifică setările în fereastra **Antivirus pentru Web**.  
După ce configurezi un nivel particularizat de securitate a traficului Web, numele nivelului de securitate din secțiunea **Nivel de securitate** devine **Particularizat**.
- Dacă dorești ca nivelul de securitate a traficului Web să devină cel **Recomandat**, fă clic pe butonul **Implicit**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Schimbarea acțiunii de efectuat asupra obiectelor de trafic Web rău intenționate

*Pentru a schimba acțiunea de efectuat asupra obiectelor de trafic Web rău intenționate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.
3. În secțiunea **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze asupra obiectelor de trafic Web rău intenționate:
  - **Selectare automată acțiune.**
  - **Blocare descărcare.**
  - **Permitere descărcare.**
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Scanarea cu Antivirusul pentru Web a adreselor URL în bazele de date cu adrese Web periculoase și de phishing

Scanarea linkurilor pentru a vedea dacă acestea sunt incluse în lista de adrese Web de phishing permite evitarea *atacurilor de tip phishing*. Un atac de tip phishing poate fi deghizat, de exemplu, într-un mesaj de e-mail de la bancă în care este inclus un link către site-ul Web oficial al băncii respective. Dacă faci clic pe link, vei fi direcționat către o copie fidelă a site-ului Web al băncii, browserul afișând inclusiv adresa Web reală a băncii, chiar dacă tu ai accesat un site falsificat. Începând din acest moment, toate acțiunile pe care le faci pe site sunt urmărite și pot fi utilizate pentru a îți se sustrage bani.

Deoarece linkurile către site-uri Web de phishing pot fi primite și din alte surse decât mesajele de e-mail, precum mesajele ICQ, Antivirusul pentru Web monitorizează la nivelul traficului Web încercările de accesare a unui site Web de phishing și blochează accesul la astfel de site-uri. Listele de adrese URL de phishing sunt incluse în kitul de distribuire Kaspersky Endpoint Security.

*Pentru a configura Antivirusul pentru Web să verifice adresele URL în bazele de date cu adrese Web de phishing și periculoase:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.
3. Fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru Web**.
4. În fereastra **Antivirus pentru Web**, selectează fila **General**.
5. Efectuează următoarele acțiuni:
  - Dacă dorești ca Antivirusul pentru Web să verifice adresele URL în bazele de date cu adrese Web periculoase, în secțiunea **Metode de scanare**, bifează caseta de selectare **Verifică dacă linkurile sunt listate în baza de date de linkuri periculoase**.
  - Dacă dorești ca Antivirusul pentru Web să verifice adresele URL în bazele de date cu adrese Web de phishing, în secțiunea **Setări anti-phishing**, bifează caseta de selectare **Verifică dacă linkurile sunt listate în baza de date de linkuri de phishing**.

De asemenea, poți să verifici linkurile în bazele de date de reputație din [Kaspersky Security Network](#).

6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Utilizarea analizorului euristic cu Antivirusul pentru Web

*Pentru a configura utilizarea analizei euristice:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru Web**.
4. Selectează fila **General**.

5. Dacă dorești ca Antivirusul pentru Web să utilizeze analiza euristică pentru a scana traficul Web în vederea detectării de viruși și alte programe malware, în secțiunea **Metode de scanare**, bifează caseta de selectare **Analiză euristică pentru detectarea virușilor** și folosește cursorul pentru a seta nivelul de complexitate a analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.
6. Dacă dorești ca Antivirusul pentru Web să utilizeze analiza euristică pentru a scana pagini Web în vederea detectării de linkuri de phishing, în secțiunea **Setări anti-phishing**, bifează caseta de selectare **Analiză euristică pentru detectarea linkurilor de phishing**.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Editarea listei de adrese URL de încredere

*Pentru a crea o listă de adrese URL de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus pentru Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus pentru Web.
3. Fă clic pe butonul **Setări**.  
Se deschide fereastra **Antivirus pentru Web**.
4. Selectează fila **URL-uri de încredere**.
5. Bifează caseta de selectare **Nu se scanează traficul Web de la adresele URL de încredere**.
6. Creează o listă de adrese URL/pagini Web în al căror conținut ai încredere. Pentru a crea o listă:
  - a. Fă clic pe butonul **Adăugare**.  
De deschide fereastra **Adresă web/Mască de adresă web**.
  - b. Introdu adresa site-ului/paginii Web sau masca de adresă a site-ului/paginii Web.
  - c. Fă clic pe **OK**.  
În lista de adrese URL apare o înregistrare nouă.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Protecția traficului prin clientul MI. Antivirus IM

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre Antivirusul pentru MI și instrucțiuni despre cum se configurează setările acestei componente.

## Despre componenta Antivirus MI

Componenta Antivirus MI scanează traficul clienților de mesagerie instantanee (cunoscuți drept *clienți MI*).

Antivirusul MI nu scanează mesajele transmise prin canale criptate.

Mesajele trimise prin clienții MI pot conține următoarele tipuri de amenințări la adresa securității:

- Adrese URL prin care se încearcă descărcarea unui program rău intenționat pe computer
- Adrese URL ale unor programe și site-uri Web rău intenționate pe care intrușii le utilizează pentru atacuri de tip phishing

Scopul atacurilor de tip phishing este sustragerea datelor personale ale utilizatorilor, cum ar fi numere de cărți de credit, informații din pașaport, parole pentru sisteme de plată bancare și pentru alte servicii online (precum site-uri de rețele sociale sau conturi de e-mail).

Fișiere care pot fi transmise prin clienți MI. La încercarea de salvare a unor astfel de fișiere, acestea sunt scanate de componenta [Antivirus pentru fișiere](#).

Componenta Antivirus MI interceptează fiecare mesaj pe care utilizatorul îl trimite sau îl primește printr-un client MI și îl scanează pentru a detecta linkuri care ar putea amenința securitatea computerului:

- Dacă în mesaj nu sunt detectate URL-uri periculoase, acesta este pus la dispoziția utilizatorului.
- Dacă în mesaj sunt detectate linkuri periculoase, componenta Antivirus MI înlocuiește mesajul cu informații despre amenințare în fereastra de mesaje a clientului activ de mesagerie instantanee.





# Activarea și dezactivarea componentei Antivirus MI

Componenta Antivirus MI este activată în mod implicit, executându-se în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva componenta Antivirus MI.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Antivirus MI din fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Protecție**.  
Se deschide secțiunea **Protecție**.
4. Fă clic dreapta pe linia **Antivirus MI** pentru a afișa meniul contextual cu acțiunile acestei componente.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Antivirus MI, selectează **Pornire** în meniul contextual.  
Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus MI**, se transformă în pictograma .
  - Pentru a dezactiva componenta Antivirus MI, selectează **Oprire** în meniul contextual.  
Pictograma de stare a componentei, , care se afișează în partea stângă a liniei **Antivirus MI**, se transformă în pictograma .

*Pentru a activa sau a dezactiva componenta Antivirus MI din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus MI**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus MI.
3. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să activezi componenta Antivirus MI, bifează caseta de selectare **Activare Antivirus MI**.
- Dacă dorești să dezactivezi componenta Antivirus MI, debifează caseta de selectare **Activare Antivirus MI**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea componentei Antivirus MI

Se pot efectua următoarele acțiuni pentru configurarea componentei Antivirus MI:

- Configurarea domeniului de protecție.  
Poți extinde sau îngusta domeniul de protecție modificând tipul de mesaje client MI scanate.
- Configurarea scanării de către componenta Antivirus MI a linkurilor și a mesajelor de client MI în raport cu bazele de date de adrese Web periculoase și de phishing.

## Crearea domeniului de protecție al componentei Antivirus MI

Domeniul de protecție desemnează obiectele pe care componenta le scanează atunci când este activată. Proprietățile domeniilor de protecție diferă de la o componentă la alta. Domeniul de protecție al componentei Antivirus MI are o proprietate datorită căreia poți seta tipurile de mesaje de clienți IM, primite sau trimise, care urmează să fie scanate. În mod implicit, componenta Antivirus MI scanează atât mesajele primite, cât și pe cele trimise. Poți dezactiva scanarea traficului la ieșire.

*Pentru a crea domeniul de protecție:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus MI**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus MI.
3. În secțiunea **Domeniu de protecție**, efectuează una dintre următoarele acțiuni:
  - Dacă dorești ca Antivirusul MI să scaneze toate mesajele de client MI primite și trimise, selectează opțiunea **Mesaje primite și trimise**.
  - Dacă dorești ca Antivirusul MI să scaneze numai mesajele primite de clienți de mesagerie instantanee, selectează opțiunea **Numai mesaje primite**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.



# Scanarea adreselor URL în raport cu bazele de date periculoase și de phishing utilizând componenta Antivirus MI

*Pentru a configura componenta Antivirus MI să verifice adresele URL în raport cu bazele de date de adrese Web periculoase și de phishing:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Antivirus MI**.  
În partea dreaptă a ferestrei se afișează setările componentei Antivirus MI.
3. În secțiunea **Metode de scanare**, selectează metodele pe care dorești să le utilizeze componenta Antivirus MI:
  - Dacă dorești să verifici linkurile din mesajele clienților MI în raport cu bazele de date de adrese URL periculoase, bifează caseta de selectare **Verifică dacă linkurile sunt listate în baza de date de linkuri periculoase**.
  - Dacă dorești să verifici linkurile din mesajele clienților MI în raport cu bazele de date de adrese URL de phishing, bifează caseta de selectare **Verifică dacă linkurile sunt listate în baza de date de linkuri de phishing**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Monitorizare sistem

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre componenta Monitorizare sistem și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre componenta Monitorizare sistem


Componenta Monitorizare sistem colectează date despre acțiunile aplicațiilor de pe computer și transmite aceste informații altor componente, pentru o protecție mai bună.

## Semnăturile de șir comportamental

Semnăturile de șir comportamental (Behavior Stream Signatures, BSS) conțin secvențe de acțiuni ale aplicațiilor pe care Kaspersky Endpoint Security le clasifică drept periculoase. Dacă activitatea aplicației corespunde unei semnături de șir comportamental, Kaspersky Endpoint Security execută acțiunea specificată. Pe baza semnăturilor de șir comportamental, Kaspersky Endpoint Security oferă o apărare proactivă pentru computer.

În mod implicit, dacă activitatea aplicației corespunde unei semnături de șir comportamental, componenta Monitorizare sistem mută fișierul executabil al aplicației în [Carantină](#).

## Derularea înapoi a acțiunilor executate de programe malware

Pe baza informațiilor colectate de componenta Monitorizare sistem, Kaspersky Endpoint Security poate [derula înapoi acțiunile executate de programele malware asupra sistemului de operare](#)  în timpul executării dezinfectării.

Atunci când se derulează înapoi activitatea programelor malware în sistemul de operare, Kaspersky Endpoint Security tratează următoarele tipuri de activități ale programelor malware:

- Activitatea cu fișiere.

Kaspersky Endpoint Security șterge fișierele executabile care au fost create de un program rău intenționat și care sunt amplasate pe orice suport, cu excepția celor de rețea.

Kaspersky Endpoint Security șterge fișierele executabile care au fost create de un program în care a pătruns un program rău intenționat.

Kaspersky Endpoint Security nu restaurează fișierelor modificate sau șterse.

- Activitatea de registru.

Kaspersky Endpoint Security șterge partițiile și cheile de registru create de programele malware.

Kaspersky Endpoint Security nu restaurează partițiile și cheile de registru modificate sau șterse.

- Activitatea de sistem.

Kaspersky Endpoint Security termină procesele inițiate de un program rău intenționat.

Kaspersky Endpoint Security termină procesele în care a pătruns un program rău intenționat.

Kaspersky Endpoint Security nu reia procesele oprite de un program rău intenționat.

- Activitate de rețea.

Kaspersky Endpoint Security blochează activitatea de rețea a programelor rău intenționate.

Kaspersky Endpoint Security blochează activitatea de rețea a proceselor în care a pătruns un program rău intenționat.

O restaurare a acțiunilor unui program periculos poate fi inițiată de componenta [Antivirus pentru fișiere](#) sau în cursul unei [scanări de viruși](#).

Derularea înapoi a operațiunilor programelor malware afectează un set de date strict definit. Restaurarea nu are efecte adverse asupra sistemului de operare sau asupra integrității datelor computerului tău.

## Activare și dezactivare Monitorizare sistem

În mod implicit, componenta Monitorizare sistem este activată și se execută în modul recomandat de Kaspersky. Dacă este necesar, poți dezactiva componenta Monitorizare sistem.

Nu se recomandă dezactivarea componentei Monitorizare sistem decât dacă este absolut necesar, deoarece aceasta ar afecta performanțele componentelor protecției. Componentele protecției pot solicita date colectate de către componenta Monitorizare sistem pentru a identifica mai precis o amenințare detectată.



Componenta Monitorizare sistem poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)


*Pentru a activa sau a dezactiva componenta Monitorizare sistem în fila **Protecție și control** din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Protecție**.  
Se deschide secțiunea **Protecție**.
4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Monitorizare sistem.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa componenta Monitorizare sistem, selectează **Pornire**.

Pictograma de stare a componentei , care se afișează în stânga liniei **Monitorizare sistem**, se schimbă în pictograma .

- Pentru a dezactiva componenta Monitorizare sistem, selectează **Oprire**.

Pictograma de stare a componentei , care se afișează în stânga liniei **Monitorizare sistem**, se schimbă în pictograma .

*Pentru a activa sau a dezactiva componenta Monitorizare sistem din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Monitorizare sistem**.  
În partea dreaptă a ferestrei se afișează setările componentei **Monitorizare sistem**.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Monitorizare sistem, bifează caseta de selectare **Activare Monitorizare sistem**.
  - Pentru a dezactiva componenta Monitorizare sistem, debifează caseta de selectare **Activare Monitorizare sistem**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea componentei Monitorizare sistem

Poți efectua următoarele acțiuni pentru configurarea componentei System Watcher:

- activarea sau dezactivarea protecției împotriva exploiturilor;
- alegerea acțiunii de efectuat la detectarea unei activități rău intenționate într-un program;
- activarea sau dezactivarea derulării înapoi a acțiunilor programelor malware în timpul dezinfectării.

## Activarea sau dezactivarea protecției împotriva exploiturilor

*Pentru a activa sau a dezactiva protecția împotriva [exploiturilor](#):*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Monitorizare sistem**.

În partea dreaptă a ferestrei se afișează setările componentei **Monitorizare sistem**.

3. Efectuează una dintre următoarele acțiuni:

- Bifează caseta de selectare **Activare prevenire exploatare** dacă dorești ca aplicația Kaspersky Endpoint Security să monitorizeze fișierele utilizate de programele vulnerabile la lansarea lor.

Dacă aplicația Kaspersky Endpoint Security detectează că un fișier utilizat de un program vulnerabil a fost lansat de altceva decât utilizatorul, va acționa în conformitate cu selecția ta din lista pop-up **Acțiune la detectarea amenințării**.

- Bifează caseta de selectare **Activare prevenire exploatare** dacă dorești ca aplicația Kaspersky Endpoint Security să monitorizeze fișierele utilizate de programele vulnerabile la lansarea lor.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Alegerea acțiunii de efectuat la detectarea unei activități rău intenționate într-un program

*Pentru a alege ce trebuie făcut dacă un program efectuează o activitate rău intenționată, parcurge următorii pași:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Monitorizare sistem**.

În partea dreaptă a ferestrei se afișează setările componentei **Monitorizare sistem**.

3. În secțiunea **Acțiune la detectarea amenințării** din lista pop-up **La detectarea activității programelor malware**, alege următoarea acțiune:

- **Selectare automată acțiune.**
- **Mută fișierul în Carantină.**
- **Terminare program periculos.**
- **Omitere.**

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea și dezactivarea restaurării acțiunilor programelor periculoase în timpul dezinfectării

*Pentru a activa sau a dezactiva derularea înapoi a acțiunilor programelor malware în timpul dezinfectării:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Monitorizare sistem**.  
În partea dreaptă a ferestrei se afișează setările componentei **Monitorizare sistem**.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să deruleze înapoi acțiunile efectuate de programele malware asupra sistemului de operare în timpul executării dezinfectării, bifează caseta de selectare **Restaurare a acțiunilor programului malware în timpul dezinfectării**.
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să ignore acțiunile efectuate de programele malware asupra sistemului de operare în timpul executării dezinfectării, debifează caseta de selectare **Restaurare a acțiunilor programului malware în timpul dezinfectării**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Firewall

Această secțiune conține informații despre componenta Firewall și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre Firewall

În timp ce utilizează rețele LAN și Internetul, un computer este expus la viruși, alte programe malware și o varietate de atacuri care exploatează vulnerabilitățile sistemelor de operare și ale software-ului.

Componenta Firewall protejează datele personale stocate pe computerul utilizatorului, blocând majoritatea posibilelor amenințări pentru sistemul de operare, cât timp computerul este conectat la Internet sau la o rețea locală. Firewall detectează toate conexiunile de rețea ale computerului utilizatorului și furnizează o listă de adrese IP, indicând starea conexiunii de rețea implicite.

Componenta Firewall filtrează toată activitatea de rețea potrivit [regulilor de rețea](#). Configurarea regulilor de rețea îți permite să specifice nivelul dorit de protecție a computerului, mergând de la blocarea accesului la Internet pentru toate aplicațiile până la permiterea unui acces nelimitat.

## Activarea sau dezactivarea Firewall





În mod implicit, Firewall este activat și funcționează într-un mod optim. Dacă este nevoie, poți dezactiva Firewall.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Firewall în fila Protecție și control din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Protecție**.  
Se deschide secțiunea **Protecție**.
4. Fă clic dreapta pe linia **Firewall** pentru a deschide meniul contextul al acțiunilor Firewall.
5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa Firewall, în meniul contextual, selectează **Pornire**.  
Pictograma de stare a componentei , care se afișează în stânga liniei **Firewall**, se schimbă în pictograma .
- Pentru a dezactiva Firewall, în meniul contextual, selectează **Opre**.  
Pictograma de stare a componentei , care se afișează în stânga liniei **Firewall**, se schimbă în pictograma .

*Pentru a activa sau a dezactiva componenta Firewall, în fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează **Firewall**.  
În partea dreaptă a ferestrei se afișează setările componentei Firewall.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa Firewall, bifează caseta de selectare **Activare Firewall**.
  - Pentru a dezactiva Firewall, bifează caseta de selectare **Dezactivare Firewall**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Despre regulile de rețea

*Regulile de rețea* reprezintă acțiuni de permitere sau de blocare efectuate de componenta Firewall la detectarea unei încercări de conectare la rețea.

Componenta Firewall furnizează protecție împotriva atacurilor de rețea de diferite tipuri la două niveluri: la nivel de rețea și la nivel de program. Protecția la nivel de rețea este asigurată prin aplicarea regulilor pentru pachete de rețea. Protecția la nivel de program este asigurată prin aplicarea regulilor conform cărora aplicațiile instalate pot accesa resursele de rețea.

În funcție de cele două niveluri ale protecției Firewall, poți crea:

- *Reguli pentru pachete de rețea.* Regulile pentru pachete de rețea impun restricții asupra pachetelor de rețea indiferent de program. Astfel de reguli restricționează traficul de rețea la intrare și la ieșire desfășurat prin anumite porturi ale protocolului de date selectat. Componenta Firewall specifică în mod implicit anumite reguli pentru pachete de rețea.
- *Reguli de rețea ale aplicației.* Regulile de rețea pentru aplicație impun restricții asupra activității de rețea a unei anumite aplicații. Ele iau în calcul nu numai caracteristicile pachetului de rețea, dar și aplicația căreia îi este adresat sau cea care a emis acest pachet de rețea. Aceste reguli fac posibilă filtrarea detaliată a activităților de rețea: de exemplu, atunci când un anumit tip de conexiune de rețea este blocat pentru unele aplicații, dar este permis pentru altele.

Regulile pentru pachete de rețea au o prioritate mai mare decât regulile de rețea pentru aplicații. Dacă pentru același tip de activitate de rețea sunt specificate atât reguli pentru pachete de rețea, cât și reguli de rețea pentru aplicații, activitatea de rețea este tratată conform regulilor pentru pachete de rețea.

Poți specifica o prioritate de executare pentru fiecare regulă pentru pachete de rețea și pentru fiecare regulă de rețea pentru aplicații.

Regulile pentru pachete de rețea au o prioritate mai mare decât regulile de rețea pentru aplicații. Dacă pentru același tip de activitate de rețea sunt specificate atât reguli pentru pachete de rețea, cât și reguli de rețea pentru aplicații, activitatea de rețea este tratată conform regulilor pentru pachete de rețea.

Regulile de rețea pentru aplicații funcționează după cum urmează: o regulă de rețea pentru aplicații include reguli de acces bazate pe starea rețelei: *publică*, *locală* sau *de încredere*. De exemplu, aplicațiilor din grupul de încredere Restrictionat la nivel superior nu le este permisă, mod implicit, nicio activitate de rețea în rețele cu toate stările. Dacă o regulă de rețea este specificată pentru o aplicație individuală (aplicație principală), atunci procesele secundare ale altor aplicații vor fi executate conform regulii de rețea a aplicației principale. Dacă nu există o regulă de rețea pentru aplicație, procesele secundare vor fi executate conform regulii de acces la rețea a grupului de încredere al aplicației.



De exemplu, ați interzis orice activitate de rețea în rețele cu toate stările pentru toate aplicațiile, cu excepția browserului X. Dacă începeți instalarea browserului Y (proces secundar) din browserul X (aplicația principală), atunci instalatorul browserului Y va accesa rețeaua și va descărca fișierele necesare. După instalare, browserului Y i se va refuza orice conexiuni la rețea conform setărilor Firewall. Pentru a interzice activitatea de rețea a instalatorului browserului Y ca proces secundar, trebuie să adăugați o regulă de rețea pentru instalatorul browserului Y.

## Despre starea conexiunii de rețea

Firewall controlează toate conexiunile de rețea de pe computerul utilizatorului și atribuie automat o stare fiecărei conexiuni de rețea.

Conexiunea de rețea poate avea una dintre următoarele patru tipuri de stare:

- **Rețea publică.** Această stare este pentru rețele care nu sunt protejate de nicio aplicație antivirus, de niciun firewall sau filtru (de exemplu, rețelele din Internet cafe-uri). Când utilizatorul folosește un computer conectat la o astfel de rețea, Firewall blochează accesul la fișierele și imprimantele acestui computer. Utilizatorii externi nu pot accesa, de asemenea, date prin directoare partajate și acces la distanță la desktopul acestui computer. Firewall filtrează activitatea de rețea a fiecărei aplicații potrivit regulilor de rețea setate pentru ea.  
Firewall atribuie în mod implicit starea *Rețea publică* întregului Internet. Nu poți modifica starea pentru Internet.
- **Rețea locală.** Această stare este atribuită rețelelor în ai căror utilizatori se are încredere în privința accesului la fișierele și imprimantele de pe acest computer (de exemplu, un LAN sau o rețea de domiciliu).
- **Rețea de încredere.** Această stare este destinată unei rețele sigure în care computerul nu este expus la atacuri sau încercări neautorizate de accesare a datelor. Firewall permite orice activitate de rețea în rețelele cu această stare.

## Modificarea stării conexiunii de rețea

*Pentru a schimba starea unei conexiuni de rețea:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.  
În partea dreaptă a ferestrei se afișează setările componentei Firewall.
3. Fă clic pe butonul **Rețele disponibile**.  
Se deschide fereastra **Firewall**.
4. Selectează conexiunea de rețea a cărei stare dorești să o modifice.

5. În meniul contextual, selectează [starea conexiunii de rețea](#):

- **Rețea publică.**
- **Rețea locală.**
- **Rețea de încredere.**

6. În fereastra **Firewall**, fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Gestionarea regulilor pentru pachetele de rețea

Poți executa următoarele acțiuni atunci când gestionezi regulile pentru pachetele de rețea:

- Creează o regulă nouă pentru pachete de rețea.

Poți crea o regulă nouă pentru pachete de rețea creând un set de condiții și de acțiuni care se aplică pachetelor de rețea și fluxurilor de date.

- Activează sau dezactivează o regulă pentru pachete de rețea.

Toate regulile pentru pachete de rețea create de Firewall au în mod implicit starea *Activat*. Atunci când o regulă pentru pachete de rețea este activată, Firewall aplică această regulă.

Poți dezactiva orice regulă pentru pachete de rețea selectată în lista de reguli pentru pachete de rețea. Atunci când o regulă pentru pachete de rețea este dezactivată, Firewall nu aplică temporar această regulă.

O regulă nouă particularizată pentru pachete de rețea este adăugată la lista de reguli pentru pachete de rețea cu starea *Activată* în mod implicit.

- Editează setările unei reguli pentru pachete de rețea existente.

După ce creezi o regulă nouă pentru pachete de rețea, poți reveni oricând la editarea setărilor sale și le poți modifica după cum este nevoie.

- Modifică acțiunea Firewall pentru o regulă pentru pachete de rețea.

În lista de reguli pentru pachete de rețea, poți edita acțiunea luată de Firewall la detectarea unei activități de rețea care corespunde unei anumite reguli pentru pachete de rețea.

- Modifică prioritatea unei reguli pentru pachete de rețea.

Poți mări sau scădea prioritatea unei reguli pentru pachete de rețea care este selectată în listă.

- Elimină o regulă pentru pachete de rețea.

Poți elimina o regulă pentru pachete de rețea pentru a opri aplicarea regulii respective de către Firewall la detectarea unei activități de rețea și pentru a opri afișarea acestei reguli în lista de reguli pentru pachete de rețea cu starea *Dezactivată*.

## Crearea și editarea unei reguli pentru pachete de rețea

La crearea de reguli pentru pachete de rețea, reține faptul că acestea au o prioritate mai mare decât regulile de rețea pentru aplicații.

*Pentru a crea sau a edita o regulă pentru pachete de rețea:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează **Firewall**.
3. Fă clic pe butonul **Reguli pachet rețea**.
4. Fereastra **Firewall** se deschide în fila **Reguli pachet rețea**.  
Această filă afișează o listă de reguli implicite pentru pachete de rețea; aceste reguli sunt setate de componenta Firewall.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a crea o regulă nouă pentru pachete de rețea, fă clic pe butonul **Adăugare**.
  - Pentru a edita o regulă pentru pachete de rețea, selectează regula în lista de reguli pentru pachete de rețea și fă clic pe butonul **Editare**.

Se deschide fereastra **Regulă de rețea**.

6. În lista verticală **Acțiune**, selectează acțiunea de efectuat de componenta Firewall la detectarea acestui tip de activitate de rețea:
  - **Permitere**
  - **Blocare**
  - **După regulile de aplicații**.
7. În câmpul **Nume**, specifică numele [serviciului de rețea ?](#) într-unul dintre următoarele moduri:

- Fă clic pe pictograma  din dreapta câmpului **Nume** și selectează numele serviciului de rețea din lista verticală.

Elementele din lista verticală includ servicii de rețea care definesc conexiunile de rețea utilizate cel mai frecvent.

- Introdu manual numele serviciului de rețea în câmpul **Nume**.

8. Specifică protocolul pentru transfer de date:

- a. Bifează caseta de selectare **Protocol**.

- b. În lista verticală, selectează tipul de protocol pentru care să fie monitorizată activitatea în rețea.

Componenta Firewall monitorizează conexiunile care utilizează protocoalele TCP, UDP, ICMP, ICMPv6, IGMP și GRE.

Dacă selectezi un serviciu de rețea din lista verticală **Nume**, caseta de selectare **Protocol** este bifată automat, iar lista verticală de lângă caseta de selectare conține tipul de protocol care corespunde serviciului de rețea selectat. Caseta de selectare **Protocol** este debifată în mod implicit.

9. În lista verticală **Direcție**, selectează direcția activității de rețea monitorizate.

Componenta Firewall monitorizează conexiunile de rețea care au următoarele direcții:

- **Intrare (pachet).**
- **Intrare.**
- **Intrare / Leșire**
- **Leșire (pachet).**
- **Leșire.**

10. Dacă se selectează protocolul ICMP sau ICMPv6, poți specifica tipul și codul de pachet ICMP:

- a. Bifează caseta de selectare **Tip ICMP** și selectează tipul de pachet ICMP din lista verticală.
- b. Bifează caseta de selectare **Cod ICMP** și selectează codul de pachet ICMP din lista verticală.

11. Dacă se selectează tipul de protocol TCP sau UDP, poți specifica numerele de port, delimitate prin virgulă, pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea:

- a. Introdu porturile computerului la distanță în câmpul **Porturi la distanță**.

b. Introdu porturile computerului local în câmpul **Porturi locale**.

12. În tabelul **Plăci de rețea**, specifică setările plăcilor de rețea de la care pot fi trimise pachete de rețea sau care pot primi pachete de rețea. Pentru aceasta, folosește butoanele **Adăugare**, **Editare** și **Ștergere**.

13. Dacă dorești să restricționezi controlul pachetelor de rețea pe baza valorilor lor Time to live (TTL), bifează caseta de selectare **TTL** din câmpul alăturat, specifică valorile Time to live pentru pachetele de rețea la intrare și/sau la ieșire.

O regulă de rețea va controla transmisia pachetelor de rețea pentru care valorile Time to Live nu depășesc valoarea specificată.

În caz contrar, debifează caseta de selectare **TTL**.

14. Specifică adresele de rețea ale computerelor la distanță care pot trimite și/sau primi pachete de rețea. Pentru aceasta, selectează una dintre următoarele valori în lista verticală **Adrese la distanță**:

- **Orice adresă.** Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu orice adresă IP.
- **Adrese subrețea.** Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu adrese IP asociate cu tipul de rețea selectat: **Rețele de încredere**, **Rețele locale** sau **Rețele publice**.
- **Adrese din listă.** Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu adrese IP care pot fi specificate în lista de mai jos, folosind butoanele **Adăugare**, **Editare** și **Ștergere**.

15. Specifică adresele de rețea ale computerelor pe care este instalat Kaspersky Endpoint Security și care pot trimite și/sau primi pachete de rețea. Pentru aceasta, selectează una dintre următoarele valori în lista verticală **Adrese locale**:

- **Orice adresă.** Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere pe care este instalat Kaspersky Endpoint Security și care au orice adresă IP.
- **Adrese din listă.** Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere pe care este instalat Kaspersky Endpoint Security și ale căror adrese IP pot fi specificate în lista de mai jos, folosind butoanele **Adăugare**, **Editare** și **Ștergere**.

Uneori o adresă locală nu poate fi obținută pentru aplicațiile care lucrează cu pachete de rețea. Dacă așa stau lucrurile, valoarea din setarea **Adrese locale** este ignorată.

16. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în [raport](#), bifează caseta de selectare **Înregistrare evenimente în jurnal**.

17. În fereastra **Regulă de rețea**, fă clic pe **OK**.

În cazul în care creezi o nouă regulă de rețea, aceasta se afișează în fila **Reguli pachet rețea** din fereastra **Firewall**. În mod implicit, regula nouă de rețea este amplasată la sfârșitul listei de reguli pentru pachete de rețea.

18. În fereastra **Firewall**, fă clic pe **OK**.

19. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea sau dezactivarea unei reguli pentru pachete de rețea

*Pentru a activa sau a dezactiva o regulă pentru pachete de rețea:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea  **Protecție antivirus** , selectează subsecțiunea **Firewall**.

În partea dreaptă a ferestrei se afișează setările componentei Firewall.

3. Fă clic pe butonul **Reguli pachet rețea**.

Fereastra **Firewall** se deschide în fila **Reguli pachet rețea**.

4. Selectează în listă regula pentru pachete de rețea necesară.

5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa regula, bifează caseta de selectare de lângă numele regulii de pachet de rețea.
- Pentru a dezactiva regula, debifează caseta de selectare de lângă numele regulii de pachet de rețea.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea acțiunii Firewall pentru o regulă pentru pachete de rețea

*Pentru a modifica acțiunea Firewallului aplicată unei reguli pentru pachete de rețea:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea  **Protecție antivirus** , selectează subsecțiunea **Firewall**.

În partea dreaptă a ferestrei se afișează setările componentei Firewall.

3. Fă clic pe butonul **Reguli pachet rețea**.

Fereastra **Firewall** se deschide în fila **Reguli pachet rețea**.

4. În listă, selectează regula pentru pachete de rețea a cărei acțiune dorești să o schimbi.

5. În coloana **Permisiune**, fă clic dreapta pentru a afișa meniul contextual și selectează acțiunea pe care dorești s-o atribui:

- **Permitere**
- **Blocare**
- **Conform regulii de aplicație**
- **Înregistrare evenimente în jurnal**

6. În fereastra **Firewall**, fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea priorității unei reguli pentru pachete de rețea

Prioritatea unei reguli pentru pachete de rețea este stabilită de poziția regulii în lista de reguli pentru pachete de rețea. Prioritatea cea mai mare o are regula pentru pachete de rețea din partea superioară a listei de reguli pentru pachete de rețea.

Fiecare regulă pentru pachete de rețea creată manual este adăugată la sfârșitul listei de reguli pentru pachete de rețea și are prioritatea cea mai mică.

Componenta Firewall execută regulile în ordinea în care acestea apar în lista de reguli pentru pachete de rețea, de sus în jos. În funcție de fiecare regulă pentru pachete de rețea procesată care se aplică unei anumite conexiuni de rețea, componenta Firewall fie permite, fie blochează accesul la adresa și la portul specificate în setările conexiunii de rețea respective.

*Pentru a schimba prioritatea regulii pentru pachete de rețea:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.  
În partea dreaptă a ferestrei se afișează setările componentei Firewall.
3. Fă clic pe butonul **Reguli pachet rețea**.  
Fereastra **Firewall** se deschide în fila **Reguli pachet rețea**.
4. În listă, selectează regula pentru pachete de rețea a cărei prioritate dorești să o schimbi.

5. Utilizează butoanele **Mutare sus** și **Mutare jos** pentru a muta regula de rețea în poziția dorită din lista de reguli pentru pachete de rețea.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Administrarea regulilor de rețea ale aplicației

În mod implicit, Kaspersky Endpoint Security grupează toate aplicațiile instalate pe computer după numele distribuitorului software-ului ale căror fișiere sau activități de rețea le monitorizează. Grupurile de aplicații sunt, la rândul lor, clasificate în [grupuri de încredere](#) <sup>[2]</sup>. Toate aplicațiile și grupurile de aplicații moștenesc proprietățile de la grupul lor părinte: reguli de control aplicații, reguli de rețea pentru aplicație și prioritatea în execuție.

În mod implicit, componenta Firewall aplică regulile de rețea pentru un grup de aplicații atunci când filtrează activitățile de rețea ale tuturor aplicațiilor din cadrul grupului, în mod asemănător componentei [Control drepturi aplicații](#). Regulile de rețea pentru grupurile de aplicații definesc drepturile aplicațiilor din cadrul grupului de a accesa diferite conexiuni de rețea.

În mod implicit, Firewall creează un set de reguli de rețea pentru fiecare grup de aplicații care este detectat de Kaspersky Endpoint Security pe computer. Poți modifica acțiunea Firewallului care este aplicată regulilor de rețea ale grupului de aplicații create în mod implicit. Nu poți edita, elimina, dezactiva sau modifica prioritatea regulilor de rețea pentru grupurile de aplicații care sunt create în mod implicit.

De asemenea, poți crea o regulă de rețea pentru o aplicație individuală. Această regulă va avea o prioritate mai mare decât regula de rețea pentru grupul căreia îi aparține aplicația.

Poți executa următoarele acțiuni atunci când gestionezi regulile de rețea ale aplicațiilor:

- Creează o regulă de rețea nouă.  
Poți crea o regulă de rețea nouă conform căreia componenta Firewall trebuie să reglementeze activitatea de rețea a aplicației sau a aplicațiilor care aparțin grupului de aplicații selectat.
- Activează sau dezactivează o regulă de rețea.  
Toate regulile de rețea sunt adăugate în lista de reguli de rețea pentru aplicații cu starea *Activată*. Dacă o regulă de rețea este activată, Firewall aplică această regulă.  
Poți dezactiva o regulă de rețea care a fost creată manual. Dacă o regulă de rețea este dezactivată, Firewall nu aplică temporar această regulă.
- Modifică setările unei reguli de rețea.



După ce creezi o regulă de rețea nouă, poți reveni oricând la setările sale și le poți modifica după cum este nevoie.

- Modifică acțiunea componentei Firewall pentru o regulă de rețea.

În lista de reguli de rețea, poți edita acțiunea pe care componenta Firewall o aplică pentru regula de rețea la detectarea activității de rețea a acestei aplicații sau a acestui grup de aplicații.

- Modifică prioritatea unei reguli de rețea.

Poți mări sau scădea prioritatea unei reguli de rețea particularizate.

- Șterge o regulă de rețea.

Poți șterge o regulă de rețea particularizată pentru o aplicație pentru a opri componenta Firewall să mai aplice această regulă de rețea pentru aplicația selectată sau pentru grupul de aplicații selectat la detectarea activității de rețea și pentru a opri apariția acestei reguli în lista de reguli de rețea pentru aplicație.

## Crearea și editarea unei reguli de rețea pentru o aplicație

*Pentru a crea sau a edita o regulă de rețea pentru un grup de aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.

3. Fă clic pe butonul **Reguli de rețea ale aplicației**.

Fereastra **Firewall** se deschide în fila **Reguli de control al aplicațiilor**.

4. În lista de aplicații, selectează aplicația sau grupul de aplicații pentru care dorești să creezi sau să editezi o regulă de rețea.

5. Fă clic dreapta pentru a afișa meniul contextual și selectează **Reguli de aplicații** sau **Reguli de grup**, în funcție de ce anume trebuie să faci.

Această acțiune deschide fereastra **Reguli de control al aplicațiilor** sau **Reguli pentru control grup de aplicații**.

6. În fereastra care se deschide, selectează fila **Reguli rețea**.

7. Efectuează una dintre următoarele acțiuni:


- Pentru a crea o regulă de rețea nouă, fă clic pe butonul **Adăugare**.
- Pentru a edita o regulă de rețea, selectează regula în lista de reguli de rețea și fă clic pe butonul **Editare**.

Se deschide fereastra **Regulă de rețea**.

8. În lista verticală **Acțiune**, selectează acțiunea de efectuat de componenta Firewall la detectarea acestui tip de activitate de rețea:

- **Permitere**
- **Blocare**

9. În câmpul **Nume**, specifică numele serviciului de rețea într-unul dintre următoarele moduri:

- Fă clic pe pictograma  din dreapta câmpului **Nume** și selectează numele serviciului de rețea din lista verticală.

Elementele din lista verticală includ servicii de rețea care definesc conexiunile de rețea utilizate cel mai frecvent.

- Introdu manual numele serviciului de rețea în câmpul **Nume**.

10. Specifică protocolul pentru transfer de date:

a. Bifează caseta de selectare **Protocol**.

b. În lista verticală, selectează tipul de protocol pentru care să fie monitorizată activitatea de rețea.

Componenta Firewall monitorizează conexiunile care utilizează protocoalele TCP, UDP, ICMP, ICMPv6, IGMP și GRE.

Dacă selectezi un serviciu de rețea din lista verticală **Nume**, caseta de selectare **Protocol** este bifată automat, iar lista verticală de lângă caseta de selectare conține tipul de protocol care corespunde serviciului de rețea selectat. Caseta de selectare **Protocol** este debifată în mod implicit.

11. În lista verticală **Direcție**, selectează direcția activității de rețea monitorizate.

Componenta Firewall monitorizează conexiunile de rețea care au următoarele direcții:

- **Intrare**.
- **Intrare/Ieșire**.
- **Ieșire**.

12. Dacă se selectează protocolul ICMP sau ICMPv6, poți specifica tipul și codul de pachet ICMP:

a. Bifează caseta de selectare **Tip ICMP** și selectează tipul de pachet ICMP din lista verticală.

- b. Bifează caseta de selectare **Cod ICMP** și selectează codul de pachet ICMP din lista verticală.
13. Dacă se selectează tipul de protocol TCP sau UDP, poți specifica numerele de port, delimitate prin virgulă, pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea:
- a. Introdu porturile computerului la distanță în câmpul **Porturi la distanță**.
- b. Introdu porturile computerului local în câmpul **Porturi locale**.
14. Specifică adresele de rețea ale computerelor la distanță care pot trimite și/sau primi pachete de rețea. Pentru aceasta, selectează una dintre următoarele valori în lista verticală **Adrese la distanță**:
- **Orice adresă**. Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu orice adresă IP.
  - **Adrese subrețea**. Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu adrese IP asociate cu tipul de rețea selectat: **Rețele de încredere**, **Rețele locale** sau **Rețele publice**.
  - **Adrese din listă**. Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere la distanță cu adrese IP care pot fi specificate în lista de mai jos, folosind butoanele **Adăugare**, **Editare** și **Ștergere**.
15. Specifică adresele de rețea ale computerelor pe care este instalat Kaspersky Endpoint Security și care pot trimite și/sau primi pachete de rețea. Pentru aceasta, selectează una dintre următoarele valori în lista verticală **Adrese locale**:
- **Orice adresă**. Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere pe care este instalat Kaspersky Endpoint Security și care au orice adresă IP.
  - **Adrese din listă**. Regula de rețea controlează pachetele de rețea trimite și/sau primite de computere pe care este instalat Kaspersky Endpoint Security și ale căror adrese IP pot fi specificate în lista de mai jos, folosind butoanele **Adăugare**, **Editare** și **Ștergere**.
- Uneori o adresă locală nu poate fi obținută pentru aplicațiile care lucrează cu pachete de rețea. Dacă așa stau lucrurile, valoarea din setarea **Adrese locale** este ignorată.
16. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în [raport](#), bifează caseta de selectare **Înregistrare evenimente în jurnal**.
17. În fereastra **Regulă de rețea**, fă clic pe **OK**.

Dacă ai creat o regulă de rețea nouă, aceasta se afișează în fila **Reguli rețea**.

18. Fă clic pe **OK** în fereastra **Reguli pentru control grup de aplicații** dacă regula este destinată unui grup de aplicații sau în fereastra **Reguli de control al aplicațiilor** dacă regula este destinată unei aplicații.

19. În fereastra **Firewall**, fă clic pe **OK**.

20. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea și dezactivarea unei reguli de rețea pentru o aplicație

*Pentru a activa sau a dezactiva o regulă de rețea pentru o aplicație:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.

În partea dreaptă a ferestrei se afișează setările componentei Firewall.

3. Fă clic pe butonul **Reguli de rețea ale aplicației**.

Fereastra **Firewall** se deschide în fila **Reguli de control al aplicațiilor**.

4. În listă, selectează aplicația sau grupul de aplicații pentru care dorești să activezi sau să dezactivezi o regulă de rețea.

5. Fă clic dreapta pentru a afișa meniul contextual și selectează **Reguli de aplicații** sau **Reguli de grup**, în funcție de ce anume trebuie să faci.

Această acțiune deschide fereastra **Reguli de control al aplicațiilor** sau **Reguli pentru control grup de aplicații**.

6. În fereastra care se deschide, selectează fila **Reguli rețea**.

7. În lista de reguli de rețea pentru un grup de aplicații, selectează regula de rețea relevantă.

8. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să activezi regula, bifează caseta de selectare de lângă numele regulii de rețea.
- Dacă dorești să dezactivezi regula, debifează caseta de selectare de lângă numele regulii de rețea.

Nu poți dezactiva o regulă de rețea pentru un grup de aplicații care este creată de Firewall în mod implicit.

9. Fă clic pe **OK** în fereastra **Reguli pentru control grup de aplicații** dacă regula este destinată unui grup de aplicații sau în fereastra **Reguli de control al aplicațiilor** dacă regula este destinată unei aplicații.
10. În fereastra **Firewall**, fă clic pe **OK**.
11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea acțiunii Firewall pentru o regulă de rețea pentru o aplicație

Poți modifica acțiunea pe care componenta Firewall o aplică tuturor regulilor de rețea pentru o aplicație sau un grup de aplicații care au fost create în mod implicit și poți modifica acțiunea pe care componenta Firewall o aplică pentru o regulă de rețea individuală particularizată pentru o aplicație sau un grup de aplicații.

*Pentru a modifica acțiunea componentei Firewall pentru toate regulile de rețea pentru o aplicație sau un grup de aplicații:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.  
În partea dreaptă a ferestrei se afișează setările componentei Firewall.
3. Fă clic pe butonul **Reguli de rețea ale aplicației**.  
Fereastra **Firewall** se deschide în fila **Reguli de control al aplicațiilor**.
4. Dacă dorești să modifice acțiunea aplicată de componenta Firewall tuturor regulilor de rețea care sunt create în mod implicit, selectează o aplicație sau un grup de aplicații în listă. Regulile de rețea create manual rămân nemodificate.
5. În coloana **Rețea**, fă clic pentru a afișa meniul contextual și selectează acțiunea pe care dorești s-o atribui:
  - **Moștenire**
  - **Permitere**
  - **Blocare**
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

*Pentru a modifica răspunsul componentei Firewall pentru o regulă de rețea pentru o aplicație sau un grup de aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează **Firewall**.

În partea dreaptă a ferestrei se afișează setările componentei Firewall.

3. Fă clic pe butonul **Reguli de rețea ale aplicației**.

Fereastra **Firewall** se deschide în fila **Reguli de control al aplicațiilor**.

4. În listă, selectează aplicația sau grupul de aplicații pentru care dorești să modifice acțiunea pentru o regulă de rețea.

5. Fă clic dreapta pentru a afișa meniul contextual și selectează **Reguli de aplicații** sau **Reguli de grup**, în funcție de ce anume trebuie să faci.

Această acțiune deschide fereastra **Reguli de control al aplicațiilor** sau **Reguli pentru control grup de aplicații**.

6. În fereastra care se deschide, selectează fila **Reguli rețea**.

7. Selectează regula de rețea pentru care dorești să modifice acțiunea componentei Firewall.

8. În coloana **Permisiune**, fă clic dreapta pentru a afișa meniul contextual și selectează acțiunea pe care dorești s-o atribui:

- **Permitere**
- **Blocare**
- **Înregistrare evenimente în jurnal**

9. Fă clic pe **OK** în fereastra **Reguli pentru control grup de aplicații** dacă regula este destinată unui grup de aplicații sau în fereastra **Reguli de control al aplicațiilor** dacă regula este destinată unei aplicații.

10. În fereastra **Firewall**, fă clic pe **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea priorității unei reguli de rețea pentru o aplicație

Prioritatea unei reguli de rețea este determinată de poziția sa în lista de reguli de rețea. Firewall execută regulile în ordinea în care ele apar în lista de reguli de rețea, de sus în jos. Potrivit fiecărei reguli de rețea procesate care se aplică unei anumite conexiuni de rețea, Firewall permite sau blochează accesul de rețea către adresa și portul indicate în setările acestei conexiuni de rețea.

Regulile de rețea create manual au o prioritate mai mare decât regulile de rețea implicite.

Nu poți modifica prioritatea regulilor de rețea pentru grupurile de aplicații care sunt create în mod implicit.

*Pentru a modifica prioritatea unei reguli de rețea:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Firewall**.  
În partea dreaptă a ferestrei se afișează setările componentei Firewall.
3. Fă clic pe butonul **Reguli de rețea ale aplicației**.  
Fereastra **Firewall** se deschide în fila **Reguli de control al aplicațiilor**.
4. În lista de aplicații, selectează aplicația sau grupul de aplicații pentru care dorești să modifice prioritatea pentru o regulă de rețea.
5. Fă clic dreapta pentru a afișa meniul contextual și selectează **Reguli de aplicații** sau **Reguli de grup**, în funcție de ce anume trebuie să faci.  
Această acțiune deschide fereastra **Reguli de control al aplicațiilor** sau **Reguli pentru control grup de aplicații**.
6. În fereastra care se deschide, selectează fila **Reguli rețea**.
7. Selectează regula de rețea a cărei prioritate dorești să o modifice.
8. Utilizează butoanele **Mutare sus** și **Mutare jos** pentru a muta regula de rețea în poziția dorită din lista de reguli de rețea.
9. Fă clic pe **OK** în fereastra **Reguli pentru control grup de aplicații** dacă regula este destinată unui grup de aplicații sau în fereastra **Reguli de control al aplicațiilor** dacă regula este destinată unei aplicații.
10. În fereastra **Firewall**, fă clic pe **OK**.
11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Monitor rețea

Această secțiune conține informații despre componenta Monitor rețea și instrucțiuni despre cum să o porniți.

## Despre Monitor rețea

*Monitor rețea* este un instrument destinat vizualizării în timp real a informațiilor despre activitatea de rețea a computerului unui utilizator.

## Pornirea instrumentului Monitor rețea

*Pentru a porni instrumentul Monitor rețea:*

1. Deschide [fereastra principală a aplicației](#).

2. Selectează fila **Protecție și control**.

3. Fă clic pe secțiunea **Protecție**.

Se deschide secțiunea **Protecție**.

4. Fă clic dreapta pe linia **Firewall** pentru a deschide meniul contextul al operațiunilor Firewall.

5. În meniul contextual, selectează **Monitorizare rețea**.

Se deschide fereastra **Monitorizare rețea**. Informațiile despre activitatea de rețea a computerului sunt afișate în cele patru file ale acestei ferestre:

- Fila **Activitate rețea** afișează toate conexiunile de rețea active în prezent pe computer. Se afișează atât conexiunile de rețea la ieșire, cât și cele la intrare.
- Fila **Porturi deschise** listează toate porturile de rețea deschise ale computerului.
- Fila **Trafic de rețea** afișează volumul de trafic de rețea la intrare și la ieșire între computerul utilizatorului și celelalte computere din rețeaua la care utilizatorul este conectat în prezent.
- Fila **Computere blocate** listează adresele IP ale computerelor la distanță a căror activitate de rețea a fost blocată de componenta Blocare atacuri de rețea după detectarea încercărilor de atacuri de rețea inițiate de la aceste adrese IP.

## Blocare atacuri de rețea

Această secțiune conține informații despre componenta Blocare atacuri de rețea și instrucțiuni despre configurarea setărilor pentru această componentă.



## Despre componenta Blocare atacuri de rețea

Componenta Blocare atacuri de rețea scanează traficul de rețea de la intrare, căutând activitate tipică atacurilor de rețea. Atunci când este detectată o încercare de atac de rețea care are drept țintă calculatorul tău, Kaspersky Endpoint Security blochează activitatea de rețea de la computerul agresor. Pe ecran ți se afișează o notificare privind atacul de rețea încercat, care conține informații despre computerul agresor.

Traficul de rețea de la computerul agresor este blocat pentru o oră. Poți edita setările pentru blocarea unui computer agresor.

Descrierile tipurilor de atacuri de rețea cunoscute în prezent și ale modurilor de combatere sunt furnizate în bazele de date Kaspersky Endpoint Security. Lista de atacuri de rețea pe care le detectează componenta Blocare atacuri de rețea este actualizată în cursul [actualizărilor bazelor de date și modulelor aplicației](#).

## Activarea și dezactivarea Blocare atacuri de rețea

Componenta Blocare atacuri de rețea este activată în mod implicit, funcționând în modul optim. Dacă este necesar, poți dezactiva componenta Blocare atacuri de rețea.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Blocare atacuri de rețea, efectuează următoarele acțiuni în fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.

2. Selectează fila **Protecție și control**.



3. Fă clic pe secțiunea **Protecție**.

Se deschide secțiunea **Protecție**.



4. Fă clic dreapta pe linia **Blocare atacuri de rețea** pentru a afișa meniul contextual al acțiunilor componentei Blocare atacuri de rețea.

5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa componenta Blocare atacuri de rețea, selectează **Pornire** în meniul contextual.

Pictograma de stare a componentei, , care se afișează în stânga liniei **Blocare atacuri de rețea**, se transformă în pictograma .

- Pentru a dezactiva componenta Blocare atacuri de rețea, selectează **Oprire** în meniul contextual.

Pictograma de stare a componentei, , care se afișează în stânga liniei **Blocare atacuri de rețea**, se transformă în pictograma .

*Pentru a activa sau a dezactiva componenta Blocare atacuri de rețea în fereastra principală a aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Blocare atacuri de rețea**.  
Setările componentei Blocare atacuri de rețea se afișează în partea dreaptă a ferestrei.
3. Efectuează următoarele acțiuni:
  - Pentru a activa componenta Blocare atacuri de rețea, bifează caseta de selectare **Activare Blocare atacuri de rețea**.
  - Pentru a dezactiva componenta Blocare atacuri de rețea, debifează caseta de selectare **Activare Blocare atacuri de rețea**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Setările componentei Blocare atacuri de rețea

Se pot efectua următoarele acțiuni pentru configurarea setărilor componentei Blocare atacuri de rețea:

- Configurarea setărilor folosite la blocarea unui computer atacator.
- Generarea unei liste de adrese pentru excluderi de la blocare.

## Editarea setărilor folosite la blocarea unui computer atacator

*Pentru a edita setările pentru blocarea unui computer agresor:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Blocare atacuri de rețea**.  
Setările componentei Blocare atacuri de rețea se afișează în partea dreaptă a ferestrei.

3. Bifează caseta de selectare **Adăugare computer agresor la lista de computere blocate pentru**.

Dacă această casetă de selectare este bifată, la detectarea unei încercări de atac de rețea, componenta Blocare atacuri de rețea blochează traficul de rețea dinspre computerul agresor o perioadă de timp egală cu cea specificată de tine. Acest lucru protejează automat computerul împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă.

Dacă această casetă de selectare este debifată, la detectarea unei încercări de atac de rețea, componenta Blocare atacuri de rețea nu activează protecția automată împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă.

4. În câmpul de lângă caseta de selectare **Adăugare computer agresor la lista de computere blocate pentru** poți schimba perioada de timp în decursul căreia computerul agresor să fie blocate.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea adreselor de excluderi de la blocare

*Pentru a configura adresele de excluderi de la blocare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Blocare atacuri de rețea**.

Setările componentei Blocare atacuri de rețea se afișează în partea dreaptă a ferestrei.

3. Fă clic pe butonul **Excluderi**.

Se deschide fereastra **Excluderi**.

4. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să creezi o adresă IP nouă, fă clic pe butonul **Adăugare**.
- Dacă dorești să editezi o adresă IP adăugată anterior, selectează-o în lista de adrese și apasă pe butonul **Editare**.

Apare fereastra **Adresă IP**.

5. Introdu adresa IP a computerului de la care nu trebuie blocate atacurile de rețea.

6. În fereastra **Adresă IP**, fă clic pe **OK**.

7. În fereastra **Excluderi**, fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Prevenire atac BadUSB

Această secțiune conține informații despre componenta Prevenire atac BadUSB.

## Despre Prevenire atac BadUSB

Unii viruși modifică firmware-ul dispozitivelor USB pentru a păcăli sistemul de operare să detecteze dispozitivul USB ca tastatură.

Componenta Prevenire atac BadUSB împiedică dispozitivele USB infectate care emulează o tastatură să se conecteze la computer.

Atunci când un dispozitiv USB este conectat la computer și este identificat de aplicație drept tastatură, aplicația solicită utilizatorului să introducă un cod numeric generat de aplicație de la tastatură, folosind tastatura virtuală (dacă este disponibilă). Această procedură este cunoscută sub numele de autorizare a tastaturii. Aplicația permite utilizarea unei tastaturi autorizate și blochează o tastatură care nu a fost autorizată.

Componenta Prevenire atac BadUSB rulează în fundal imediat ce această componentă este instalată. Dacă aplicația nu se supune unei politici a Kaspersky Security Center, poți activa sau dezactiva componenta Prevenire atac BadUSB [punând în pauză temporar și reluând protecția și controlul computerului](#).

## Instalarea componentei Prevenire atac BadUSB

Dacă ai selectat [instalare de bază sau standard](#) în cursul instalării Kaspersky Endpoint Security, componenta Prevenire atac BadUSB nu este disponibilă. Pentru a o instala, trebuie să modifice setul de componente ale aplicației.

*Pentru a instala componenta BadUSB Attack Prevention:*

1. În meniul **Start**, selectează **Aplicații > Kaspersky Endpoint Security 10 for Windows > Modificare, reparare sau eliminare**.

Expertul de instalare pornește.

2. În fereastra **Modificare, reparare sau eliminare aplicație** a expertului de instalare a aplicației, fă clic pe butonul **Modificare**.

Aceasta deschide fereastra **Instalare particularizată** din Expertul de instalare a aplicației.

3. În meniul contextual al pictogramei de lângă numele componentei **Prevenire atac BadUSB**, selectează opțiunea **Caracteristica se va instala pe unitatea de hard disk locală**.

4. Fă clic pe butonul **Următorul**.

5. Urmează instrucțiunile din Expertul de instalare.

## Activarea și dezactivarea componentei Prevenire atac BadUSB

*Pentru a activa sau a dezactiva componenta Prevenire atac BadUSB:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Prevenire atac BadUSB**.  
Setările componentei Prevenire atac BadUSB se afișează în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Prevenire atac BadUSB, bifează caseta de selectare **Activare Prevenire atac BadUSB**.
  - Pentru a dezactiva componenta Prevenire atac BadUSB, debifează caseta de selectare **Activare Prevenire atac BadUSB**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Permiterea sau interzicerea utilizării tastaturii virtuale pentru autorizare

Tastatura virtuală trebuie folosită numai pentru autorizarea dispozitivelor USB care nu acceptă introducerea caracterelor aleatorii (de exemplu, scanere de coduri de bare). Nu se recomandă folosirea tastaturii virtuale pentru autorizarea dispozitivelor USB necunoscute.

*Pentru a permite sau a interzice utilizarea tastaturii virtuale pentru autorizare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Protecție antivirus**, selectează subsecțiunea **Prevenire atac BadUSB**.  
Setările componentei sunt afișate în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Bifează caseta de selectare **Interzicere utilizare tastatură vizuală pentru autorizare** pentru a bloca utilizarea tastaturii vizuale pentru autorizare.
  - Debifează caseta de selectare **Interzicere utilizare tastatură vizuală pentru autorizare** pentru a permite utilizarea tastaturii vizuale pentru autorizare.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Autorizarea tastaturii

Dispozitivele USB identificate de sistemul de operare drept tastaturi și conectate la computer înainte de instalarea componentei Prevenire atac BadUSB sunt considerate a fi autorizate după instalarea componentei.

Aplicația solicită autorizarea dispozitivului USB conectat care a fost identificat de către sistemul de operare drept tastatură numai dacă este activată solicitarea autorizării pentru tastatura USB. Utilizatorul nu poate folosi o tastatură neautorizată până când aceasta nu este autorizată.

Dacă este dezactivată solicitarea autorizării pentru tastatura USB, utilizatorul poate folosi toate tastaturile conectate. Imediat după ce este activată solicitarea autorizării pentru tastatura USB, aplicația solicită autorizarea tuturor tastaturilor neautorizate care sunt conectate.

*Pentru a autoriza o tastatură:*

1. Dacă este activată autorizarea pentru tastatura USB, conectează tastatura la un port USB.

Se deschide fereastra **<Nume tastatură> autorizare tastatură** cu detaliile tastaturii conectate și un cod numeric pentru autorizarea sa.

2. Introdu codul numeric generat aleatoriu în fereastra de autorizare de la tastatura conectată sau de la tastatura virtuală (dacă este disponibilă).
3. Fă clic pe **OK**.

Dacă a fost introdus corect codul, aplicația salvează parametrii de identificare – VID/PID pentru tastatură și numărul portului la care a fost conectată – în lista de tastaturi autorizate. Autorizarea nu trebuie repetată atunci când tastatura este reconectată sau după repornirea sistemului de operare.

Atunci când tastatura autorizată este conectată la un alt port USB al computerului, aplicația afișează din nou o solicitare de autorizare a acestei tastaturi.

Dacă a fost introdus incorect codul numeric, aplicația generează un cod nou. Sunt disponibile trei încercări pentru introducerea codului numeric. Dacă este introdus în mod incorect codul numeric de trei ori la rând sau dacă fereastra **<Nume tastatură> autorizare tastatură** este închisă, aplicația blochează introducerea de la această tastatură. Atunci când tastatura este reconectată sau după ce sistemul de operare este repornit, aplicația solicită utilizatorului să efectueze din nou autorizarea tastaturii.

## Componenta Control pornire aplicații

Această secțiune conține informații despre componenta Control pornire aplicații și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre componenta Control pornire aplicații

Componenta Control pornire aplicații monitorizează încercărilor utilizatorului de a porni aplicații și reglementează pornirea aplicațiilor folosind [regulile pentru Control la pornirea aplicației](#).

Pornirea aplicațiilor ale căror setări nu corespund niciuneia dintre regulile pentru Control la pornirea aplicației este reglementată de modul de funcționare selectat pentru componentă. În mod implicit este selectat [modul Listă neagră](#). Acest mod permite tuturor utilizatorilor să pornească toate aplicațiile.

Toate încercările utilizatorului de a porni aplicații sunt înregistrate în [rapoarte](#).

## Activarea și dezactivarea componentei Control pornire aplicații



Deși componenta Control pornire aplicații este dezactivată în mod prestabilit, o puteți activa dacă este necesar.

Această componentă poate fi activată sau dezactivată în două moduri:



- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Control pornire aplicații în fila Protecție și control din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Control endpoint**.  
Se deschide secțiunea **Control endpoint**.
4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Control pornire aplicații.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Control pornire aplicații, selectează **Pornire** în meniu.

Pictograma de stare a componentei , care se afișează în stânga liniei **Control pornire aplicații**, se transformă în pictograma .

- Pentru a dezactiva componenta Control pornire aplicații, selectează **Oprire** în meniu.

Pictograma de stare a componentei , care se afișează în stânga liniei **Control pornire aplicații**, se transformă în pictograma .

*Pentru a activa sau a dezactiva componenta Control pornire aplicații din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Control pornire aplicații, bifează caseta de selectare **Activare Control pornire aplicații**.
  - Pentru a dezactiva componenta Control pornire aplicații, debifează caseta de selectare **Activare Control pornire aplicații**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Limitările funcționalității Control pornire aplicații

Funcționalitatea componentei Control pornire aplicații este limitată în următoarele cazuri:

- Atunci când se face upgrade versiunii aplicației, importul setărilor componentei Control pornire aplicații nu este acceptat.

Pentru a restaura funcționalitatea componentei Control pornire aplicații, trebuie să reconfigurezi setările componentei.

- Dacă nu există o conexiune cu serverele KSN, Kaspersky Endpoint Security primește informații despre reputația aplicațiilor și a modulelor lor de la bazele de date locale. Dacă bazele de date locale nu conțin informații despre aplicație, aceasta nu va fi inclusă într-o categorie de grup de încredere.



Aplicațiile pot fi incluse într-o categorie diferită atunci când există o conexiune la serverele KSN, în comparație cu situația în care nu există o conexiune cu KSN.

- În baza de date Kaspersky Security Center pot fi stocate informații despre 150.000 de fișiere procesate. După atingerea acestui număr de înregistrări, nu vor mai fi procesate fișiere noi. Pentru a relua operațiunile de inventariere, trebuie să ștergi fișierele inventariate anterior în baza de date Kaspersky Security Center de pe computerul pe care este instalată aplicația Kaspersky Endpoint Security.
- Componenta nu controlează pornirea scripturilor, cu excepția cazurilor în care scriptul este trimis către interpretor prin linia de comandă.

Dacă pornirea unui interpretor este permisă de regulile pentru Control la pornirea aplicației, componenta nu va bloca un script pornit de la acest interpretor.

- Componenta nu controlează pornirea scripturi de la interpretoare neacceptate de către Kaspersky Endpoint Security.

Kaspersky Endpoint Security acceptă următoarele interpretoare:

- Java
- PowerShell

Sunt acceptate următoarele tipuri de interpretoare:

- { cCmdLineParser::itCmd, \_T("%ComSpec%") };
- { cCmdLineParser::itReg, \_T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, \_T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, \_T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, \_T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, \_T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, \_T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, \_T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, \_T("%SystemRoot%\\system32\\mmc.exe") };

- { cCmdLineParser::itMshta, \_T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, \_T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, \_T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, \_T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, \_T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, \_T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, \_T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, \_T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, \_T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, \_T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, \_T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, \_T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, \_T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, \_T("%SystemRoot%\\syswow64\\wwahost.exe") }.

## Despre regulile componenteii Control pornire aplicații

Kaspersky Endpoint Security controlează pornirea aplicațiilor de către utilizatori prin intermediul regulilor. O regulă Control la pornirea aplicației specifică condițiile de declanșare și acțiunea efectuată de componenta Control pornire aplicații atunci când regula este declanșată (permițând sau blocând pornirea aplicației de către utilizatori).

### Condiții de declanșare a regulii

O condiție pentru declanșarea regulii are următoarea corespondență: „tip condiție – criteriu condiție – valoare condiție” (vezi figura de mai jos). Pe baza condițiilor de declanșare a regulii, Kaspersky Endpoint Security aplică (sau nu aplică) o regulă unei aplicații.

**Regulă Control la pornirea aplicației**

Nume regulă:

Descriere:

**Condiții de includere:**

Criteriu condiție	Valoare condiție

+ Adăugare Editare Ștergere Conversie în excludere

**Condiții excludere:**

Criteriu condiție	Valoare condiție

+ Adăugare Editare Ștergere Conversie în condiție de includere

Coordonatori și drepturile acestora:

Coordonator	Permitere	Refuzare
Everyone	<input type="checkbox"/>	<input checked="" type="checkbox"/>

+ Adăugare Ștergere

☐ Refuză pentru alți utilizatori  
☐ Programe de actualizare de încredere

Ajutor OK Revocare

Regulă pentru Control la pornirea aplicației. Parametri condiție de declanșare a regulii

Regulile folosesc condiții de includere și de excludere:

- *Condiții de includere.* Kaspersky Endpoint Security aplică regula aplicației dacă aplicația corespunde cel puțin uneia dintre condițiile de includere.
- *Condiții de excludere.* Kaspersky Endpoint Security nu aplică regula aplicației dacă aplicația corespunde cel puțin uneia dintre condițiile de excludere și nu corespunde niciuneia dintre condițiile de includere.

Condițiile de declanșare a regulii sunt create folosind criterii. Următoarele criterii sunt folosite pentru a crea reguli în Kaspersky Endpoint Security:

- Calea către directorul care conține fișierul executabil al aplicației sau calea către fișierul executabil al aplicației.

- Metadate: nume fișier executabil al aplicației, versiune fișier executabil al aplicației, nume aplicație, versiune aplicație, vânzător aplicație.
- Codul hash al fișierului executabil al aplicației.
- Certificat: emitent, coordonator, amprentă.
- Includerea aplicației într-o categorie KL.
- Locația fișierului executabil al aplicației pe o unitate amovibilă.

Valoarea criteriului trebuie specificată pentru fiecare criteriu folosit în condiție. Dacă parametrii aplicației pornite corespund valorilor criteriilor specificate în condiția de includere, regula este declanșată. În acest caz, componenta Control pornire aplicații efectuează acțiunea prescrisă de regulă. Dacă parametrii aplicației pornite corespund valorilor criteriilor specificate în condiția de excludere, componenta Control pornire aplicații nu controlează pornirea aplicației.

## Deciziile luate de componenta Control pornire aplicații atunci când o regulă este declanșată

Atunci când o regulă este declanșată, componenta Control pornire aplicații permite utilizatorilor sau grupurilor de utilizatori să pornească aplicații sau blochează pornirea conform regulii. Poți selecta utilizatori individuali sau grupuri de utilizatori cărora li se permite sau nu li se permite să pornească aplicații care declanșează o regulă.

Dacă o regulă nu specifică utilizatorii care au permisiunea să pornească aplicații care satisfac regula, atunci această regulă este denumită regulă de *blocare*.

Dacă o regulă care nu specifică niciun utilizator care nu are permisiunea de a porni aplicații care satisfac regula, atunci această regulă este denumită regulă de *permitere*.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. De exemplu, dacă o regulă de permitere pentru componenta Control pornire aplicații a fost specificată pentru un grup de utilizatori, iar o regulă de blocare pentru componenta Control pornire aplicații a fost specificată pentru un utilizator din acest grup de utilizatori, atunci pornirea aplicației de către respectivul utilizator va fi blocată.

## Starea operațională a unei reguli

Regulile componentei Control pornire aplicații pot avea una dintre următoarele două valori de stare operațională:

- **Activat.**

Această stare operațională înseamnă că regula este activată.

- **Dezactivat.**

Această stare înseamnă că regula este dezactivată.

## Reguli implicite ale componentei Control pornire aplicații

În mod implicit, componenta Control pornire aplicații operează în modul Listă neagră. Această componentă permite tuturor utilizatorilor să pornească toate aplicațiile. Atunci când un utilizator încearcă să pornească o aplicație blocată de regulile Control la pornirea aplicației, Kaspersky Endpoint Security blochează pornirea aplicației (dacă este selectată acțiunea **Blocare**) sau salvează informații despre pornirea aplicației într-un raport (dacă este selectată acțiunea **Notificare**).

## Gestionarea regulilor componentei Control pornire aplicații

Poți executa următoarele acțiuni pentru regulile pentru Control la pornirea aplicației:

- Adăugare a unei reguli noi
- Creare sau modificare condiții pentru declanșarea unei reguli
- Editare a stării regulii

O regulă Control la pornirea aplicației poate fi activată (caseta de selectare de lângă regulă este bifată) sau dezactivată (caseta de selectare de lângă regulă este debifată). O regulă Control la pornirea aplicației este activată în mod implicit după ce este creată.

- Ștergere regulă

## Adăugarea și editarea unei reguli a componentei Control pornire aplicații

*Pentru a adăuga sau a edita o regulă a componentei Control pornire aplicații:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.
4. Efectuează una dintre următoarele acțiuni:

- Pentru a adăuga o regulă, fă clic pe butonul **Adăugare**.
- Dacă dorești să editezi o regulă existentă, selectează regula în lista de reguli și apasă pe butonul **Editare**.

Se deschide fereastra **Regulă Control la pornirea aplicației**.

5. Specifică sau editează setările pentru regulă:

- a. În câmpul **Nume regulă**, introdu sau editează numele regulii.
- b. În tabelul **Condiții de includere**, [creează](#) sau editează lista de condiții de includere care declanșează o regulă făcând clic pe butoanele **Adăugare**, **Editare**, **Ștergere** și **Conversie în excludere**.
- c. În tabelul **Condiții excludere**, creează sau editează lista de condiții de excludere care declanșează o regulă făcând clic pe butoanele **Adăugare**, **Editare**, **Ștergere** și **Conversie în condiție de includere**.
- d. Dacă este necesar, poți schimba tipul de condiție de declanșare a regulii:
  - Pentru a schimba tipul de condiție de la condiție de includere la condiție de excludere, selectează o condiție din tabelul **Condiții de includere** și fă clic pe butonul **Conversie în excludere**.
  - Pentru a schimba tipul de condiție de la condiție de excludere la condiție de includere, selectează o condiție din tabelul **Condiții excludere** și fă clic pe butonul **Conversie în condiție de includere**.
- e. Compilează sau editează o listă de utilizatori și/sau grupuri de utilizatori care au permisiunea de a lansa aplicații care îndeplinesc condițiile de declanșare a regulii. Pentru aceasta, fă clic pe butonul **Adăugare** în tabelul **Coordonatori și drepturile acestora**.

Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**. Această fereastră permite selectarea utilizatorilor și/sau a grupurilor de utilizatori.

În mod implicit, la lista de utilizatori este adăugată valoarea **Oricine**. Regula se aplică tuturor utilizatorilor.

Dacă în tabel nu este specificat niciun utilizator, regula nu poate fi salvată.

- f. În tabelul **Coordonatori și drepturile acestora**, bifează caseta de selectare **Permitere** sau **Blocare** de lângă utilizatorii și/sau grupurile de utilizatori pentru a determina dreptul lor de a porni aplicații.

Caseta de selectare bifată în mod implicit depinde de [Mod de funcționare pentru Control la pornirea aplicației](#).

- g. Bifează caseta de selectare **Refuză pentru alți utilizatori** dacă dorești ca toți utilizatorii care nu apar în coloana **Coordonator** și care nu fac parte din grupul de utilizatori specificat în coloana **Coordonator** să nu poată porni aplicațiile care corespund condițiilor de declanșare a regulii.

Când caseta de selectare **Refuză pentru alți utilizatori** este debifată, Kaspersky Endpoint Security nu controlează pornirea aplicațiilor de către utilizatori care nu sunt specificați în tabelul **Coordonatori și drepturile acestora** și care nu aparțin grupului de utilizatori specificat în tabelul **Coordonatori și drepturile acestora**.

- h. Dacă dorești ca aplicația Kaspersky Endpoint Security să considere aplicațiile care corespund condițiilor de declanșare a regulii ca fiind programe de actualizare de încredere și să le permită pornirea altor aplicații pentru care nu sunt definite reguli pentru componenta Control pornire aplicații, bifează caseta de selectare **Programe de actualizare de încredere**.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Adăugarea unei condiții de declanșare pentru o regulă a componentei Control pornire aplicații

*Pentru a adăuga o condiție nouă de declanșare pentru o regulă Control la pornirea aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.
4. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să creezi o regulă nouă și să adaugi la ea o condiție de declanșare, apasă pe butonul **Adăugare**.

- Dacă dorești să adaugi o condiție de declanșare la o regulă existentă, selectează regula în lista de regulă și apasă pe butonul **Editare**.

Se deschide fereastra **Regulă Control la pornirea aplicației**.

5. În tabelul **Condiții de includere** sau **Condiții excludere**, apasă pe butonul **Adăugare**.

Poți folosi lista derulantă a butonului **Adăugare** pentru a adăuga diferite condiții de declanșare la regulă (vezi instrucțiunile de mai jos).

*Pentru a adăuga o condiție de declanșare a regulii pe baza proprietăților fișierelor dintr-un director specificat:*

1. În lista verticală a butonului **Adăugare**, selectează **Condiție/condiții din proprietățile fișierului în directorul specificat**.

Se deschide fereastra Microsoft Windows standard **Selectare director**.

2. În fereastra **Select folder** (Selectare director), selectează un director care conține fișierele executabile ale aplicațiilor ale căror proprietăți dorești să le utilizezi ca bază pentru una sau mai multe condiții de declanșare a unei reguli.

3. Fă clic pe **OK**.

Apare fereastra **Adăugare condiție**.

4. În lista verticală **Afișare criteriu**, selectează criteriul pe baza căruia dorești să creezi una sau mai multe condiții de declanșare a regulii: **Cod hash fișier**, **Certificat**, **Categorie KL**, **Metadata** sau **Cale către director**.

Kaspersky Endpoint Security nu acceptă cod hash MD5 de fișiere și nu controlează pornirea aplicațiilor pe baza unui cod hash MD5. Drept condiție de declanșare a regulii este folosit un cod hash SHA256.

5. Dacă ai selectat **Metadata** în lista verticală **Afișare criteriu**, bifează casetele de selectare de lângă proprietățile fișierului executabil pe care dorești să le folosești în condiția de declanșare a regulii: **Nume fișier**, **Versiune fișier**, **Nume aplicație**, **Versiune aplicație** și **Furnizor**.

Dacă niciuna dintre aceste proprietăți nu este selectată, regula nu poate fi salvată.

6. Dacă ai selectat **Certificat** în lista verticală **Afișare criteriu**, bifează casetele de selectare de lângă setările pe care dorești să le folosești în condiția de declanșare a regulii: **Emitent**, **Coordonator** și **Amprentă**.

Dacă niciuna dintre aceste setări nu este selectată, regula nu poate fi salvată.



Să recomandă folosirea doar a criteriilor **Emitent** și **Coordonator** drept condiții de declanșare a regulii. Utilizarea acestor criterii nu este fiabilă.

7. Bifează casetele de selectare de lângă numele fișierelor executabile ale aplicațiilor ale căror proprietăți dorești să le incluzi în condițiile de declanșare a regulii.

8. Fă clic pe butonul **Următorul**.

Se afișează o listă de condiții definite de declanșare a regulii.

9. În lista de condiții definite de declanșare a regulii, bifează casetele de selectare de lângă condițiile de declanșare a regulii pe care dorești să le adaugi în regula componentei Control pornire aplicații.

10. Fă clic pe butonul **Terminare**.

*Pentru a adăuga o condiție de declanșare a regulii pe baza proprietăților aplicațiilor care sunt lansate pe computer:*

1. În lista verticală a butonului **Adăugare**, selectează **Condiție/condiții din proprietățile aplicațiilor pornite**.

2. În fereastra **Adăugare condiție**, în lista verticală **Afișare criteriu**, selectează criteriul pe baza căruia dorești să creezi una sau mai multe condiții de declanșare a regulii: **Cod hash fișier**, **Certificat**, **Categorie KL**, **Metadate** sau **Cale către director**.

3. Dacă ai selectat **Metadate** în lista verticală **Afișare criteriu**, bifează casetele de selectare de lângă proprietățile fișierului executabil pe care dorești să le folosești în condiția de declanșare a regulii: **Nume fișier**, **Versiune fișier**, **Nume aplicație**, **Versiune aplicație** și **Furnizor**.

Dacă niciuna dintre aceste proprietăți nu este selectată, regula nu poate fi salvată.

4. Dacă ai selectat **Certificat** în lista verticală **Afișare criteriu**, bifează casetele de selectare de lângă setările pe care dorești să le folosești în condiția de declanșare a regulii: **Emitent**, **Coordonator** și **Amprentă**.

Dacă niciuna dintre aceste setări nu este selectată, regula nu poate fi salvată.

Să recomandă folosirea doar a criteriilor **Emitent** și **Coordonator** drept condiții de declanșare a regulii. Utilizarea acestor criterii nu este fiabilă.

5. Bifează casetele de selectare de lângă numele fișierelor executabile ale aplicațiilor ale căror proprietăți dorești să le incluzi în condițiile de declanșare a regulii.

6. Fă clic pe butonul **Următorul**.

Se afișează o listă de condiții definite de declanșare a regulii.

7. În lista de condiții definite de declanșare a regulii, bifează casetele de selectare de lângă condițiile de declanșare a regulii pe care dorești să le adaugi în regula componentei Control pornire aplicații.

8. Fă clic pe butonul **Terminare**.

*Pentru a adăuga o condiție de declanșare a regulii bazate pe o categorie KL:*

1. În lista verticală a butonului **Adăugare**, selectează **Condiție/condiții "categoria KL"**.

O *categorie KL* este o listă de aplicații care partajează atribute de temă. Lista este întreținută de experții Kaspersky. De exemplu, categoria KL „Aplicații Office” include toate aplicațiile din suita Microsoft Office, Adobe Acrobat și altele.

2. În fereastra **Condiție/condiții "categoria KL"** bifează casetele de selectare de lângă numele categoriilor KL pe baza cărora dorești să creezi condițiile de declanșare a regulii.

3. Fă clic pe **OK**.

*Pentru a adăuga o condiție particularizată de declanșare a regulii:*

1. În lista verticală a butonului **Adăugare**, selectează **Condiție particularizată**.

2. În fereastra **Condiție particularizată**, apasă pe butonul **Selectare** și specifică o cale către fișierul executabil al aplicației.

3. Selectează criteriul pe baza căruia dorești să creezi o regulă de declanșare a regulii: **Cod hash fișier**, **Certificat**, **Metadata** sau **Calea către fișier sau director**.

Dacă utilizezi linkuri simbolice în câmpul **Calea către fișier sau director**, te sfătuim să rezolvi linkurile simbolice pentru funcționarea corectă a regulii Control pornire aplicații. Pentru aceasta, fă clic pe butonul **Rezolvare link simbolic**.

4. Dacă este necesar, configurează setările criteriului selectat.

5. Fă clic pe **OK**.

*Pentru a adăuga o condiție de declanșare a regulii pe baza informațiilor despre unitatea care stochează fișierul executabil al unei aplicații:*

1. În lista verticală a butonului **Adăugare**, selectează **Condiție în funcție de unitatea fișierului**.

2. În fereastra **Condiție în funcție de unitatea fișierului**, în lista verticală **Unitate**, selectează tipul de unitate pentru care pornirea aplicațiilor va servi drept condiție de declanșare a regulii.
3. Fă clic pe **OK**.

## Modificarea stării unei reguli a componentei Control pornire aplicații

*Pentru a modifica starea unei reguli a componentei Control pornire aplicații:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.
4. Selectează regula pe care dorești să o editezi.
5. În coloana **Stare**, procedează astfel:
  - Dacă dorești să activezi utilizarea unei reguli, bifează caseta de selectare de lângă regulă.
  - Dacă dorești să dezactivezi utilizarea unei reguli, debifează caseta de selectare de lângă regulă.
6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Testarea regulilor componentei Control la pornirea aplicației

Pentru a te asigura că regulile pentru Control la pornirea aplicației nu îți blochează aplicații de care ai nevoie la serviciu, se recomandă să treci în modul de testare regulile nou create și să analizezi funcționarea lor.

O analiză a funcționării regulilor pentru aplicația Control la pornirea aplicației implică examinarea evenimentelor componentei Control la pornirea aplicației care sunt raportate către Kaspersky Security Center. Dacă este permisă pornirea tuturor aplicațiilor necesare pentru activitatea utilizatorului pe computer, atunci regulile au fost create în mod corect. În caz contrar, recomandăm revizuirea setărilor pentru regulile pe care le-ai creat.

Modul de testare a regulilor pentru Control la pornirea aplicației este dezactivat în mod implicit.

*Pentru a testa regulile componentei Control la pornirea aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.
4. În lista verticală **Mod Control la pornirea aplicației**, selectează una dintre elementele următoare:
  - **Listă neagră**, dacă dorești să permiți pornirea tuturor aplicațiilor, cu excepția aplicațiilor specificate în regulile de blocare.
  - **Listă albă**, dacă dorești să blochezi pornirea tuturor aplicațiilor, cu excepția aplicațiilor specificate în regulile de permitere.
5. În lista verticală **Acțiune**, selectează **Notificare**.
6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Kaspersky Endpoint Security nu va bloca aplicațiile a căror lansare este interzisă de regulile pentru Control la pornirea aplicației, dar va trimite către serverul de administrare notificări despre pornirea lor.

## Editarea șabloanelor de mesaje aferente componentei Control pornire aplicații

Atunci când un utilizator încearcă să pornească o aplicație blocată de o regulă a componentei Control pornire aplicații, Kaspersky Endpoint Security afișează un mesaj referitor la blocarea pornirii aplicației. Dacă utilizatorul consideră că pornirea aplicației a fost blocată din greșeală, el poate utiliza linkul din mesajul text pentru a trimite un mesaj administratorului rețelei locale a companiei.

Sunt disponibile șabloane speciale pentru mesajul afișat atunci când pornirea unei aplicații este blocată și pentru mesajul care este trimis administratorului. Poți modifica șabloanele de mesaje.

*Pentru a edita un șablon de mesaj:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.

3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.
4. Fă clic pe butonul **Șabloane**.  
Se deschide fereastra **Șabloane de mesaje**.
5. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să editezi șablonul mesajului afișat la blocarea pornirii unei aplicații, selectează fila **Blocare**.
  - Dacă dorești să modifice șablonul mesajului trimis către administratorul rețelei LAN, selectează fila **Mesaj către administrator**.
6. Modifică șablonul pentru mesajul afișat atunci când pornirea unei aplicații este blocată sau mesajul care este trimis administratorului. Pentru aceasta, utilizează butoanele **Implicit** și **Variabilă**.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Despre modurile de funcționare a componentei Control pornire aplicații

Componenta Control pornire aplicații funcționează în două moduri:

- **Listă neagră.** În acest mod, componenta Control pornire aplicații permite tuturor utilizatorilor să pornească toate aplicațiile, cu excepția celor specificate în [regulile de blocare ale componentei Control pornire aplicații](#).

Acest mod al componentei Control pornire aplicații este activat în mod implicit.

- **Listă albă.** În acest mod, componenta Control pornire aplicații îi blochează pe toți utilizatorii de la pornirea tuturor aplicațiilor, cu excepția celor specificate în regulile de permitere ale componentei Control pornire aplicații.

Dacă regulile de permitere ale componentei Control pornire aplicații sunt complet configurate, componenta blochează pornirea tuturor aplicațiilor noi care nu au fost verificate de administratorul rețelei LAN, permițând însă funcționarea sistemului de operare și a aplicațiilor de încredere pe care utilizatorii se bazează în activitatea lor.

Fiecare mod are două acțiuni care pot fi luate la executarea aplicațiilor: Kaspersky Endpoint Security poate bloca pornirea aplicațiilor sau îl poate notifica pe utilizator despre pornirea unei aplicații care corespunde condițiilor din regulile componentei Control pornire aplicații.

Componenta Control pornire aplicații poate fi configurată să funcționeze în aceste moduri atât folosind interfața locală Kaspersky Endpoint Security, cât și folosind Kaspersky Security Center.

Cu toate acestea, Kaspersky Security Center oferă instrumente care nu sunt disponibile în interfața locală Kaspersky Endpoint Security, cum ar fi instrumentele care sunt necesare pentru următoarele activități:

- [Crearea categoriilor de aplicații.](#)

Regulile pentru Control la pornirea aplicației create în Consola de administrare Kaspersky Security Center se bazează pe categorii particularizate de aplicații și nu pe condițiile de includere și de excludere, ca în cazul interfeței locale Kaspersky Endpoint Security.

- [Colectarea informațiilor despre aplicațiile instalate pe computerele din rețeaua LAN.](#)

De aceea se recomandă utilizarea Kaspersky Security Center pentru a configura funcționarea componentei Control la pornirea aplicației.

## Selectarea modului pentru Control pornire aplicații

*Pentru a selecta modul pentru Control pornire aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.

3. Selectează **Activare Control pornire aplicații** pentru ca setările componentei să poată fi editate.

4. În lista verticală **Modul Control pornire aplicații**, selectează una dintre opțiunile următoare:

- **Listă neagră**, dacă dorești să permiți pornirea tuturor aplicațiilor, cu excepția aplicațiilor specificate în regulile de blocare.
- **Listă albă**, dacă dorești să blochezi pornirea tuturor aplicațiilor, cu excepția aplicațiilor specificate în regulile de permitere.

Atunci când este selectat acest mod, două reguli pentru componenta Control pornire aplicații sunt create în mod implicit: **Imagine de aur** și **Programe de actualizare de încredere**. Nu poți șterge aceste reguli. Setările acestor reguli nu pot fi editate. Poți activa sau dezactiva aceste reguli bifând sau debifând caseta de selectare de lângă regula relevantă. În mod implicit, regula **Imagine de aur** este activată, iar regula **Programe de actualizare de încredere** este dezactivată. Tuturor utilizatorilor le este permis să pornească aplicații care corespund condițiilor de declanșare din aceste reguli.

Toate regulile create în cursul modului selectat sunt salvate după modificarea modului, astfel încât regulile să poată fi refolosite. Pentru a reveni la folosirea acestor reguli, nu trebuie decât să selectezi modul necesar în lista verticală **Modul Control pornire aplicații**.

5. În lista verticală **Acțiune**, selectează acțiunea care va fi efectuată atunci când un utilizator încearcă să pornească o aplicație care este blocată de regulile Control la pornirea aplicației.
6. Bifează caseta de selectare **Monitorizare DLL și drivere** dacă dorești ca aplicația Kaspersky Endpoint Security să monitorizeze încărcarea modulelor DLL atunci când aplicațiile sunt pornite de către utilizatori.

Informațiile despre modul și aplicația care a încărcat modulul vor fi salvate într-un raport.

Dacă această casetă de selectare este bifată, modulele DLL și driverele sunt monitorizate înainte de pornirea Kaspersky Endpoint Security. Pentru a configura monitorizarea ulterioară a tuturor modulelor DLL și driverelor înainte de pornirea aplicației, repornește computerul după ce bifezi cseta de selectare **Monitorizare DLL și drivere**. Dacă nu reușești să repornești computerul, după ce bifezi caseta de selectare **Monitorizare DLL și drivere**, poți încărcă module DLL și drivere în timp ce se execută Kaspersky Endpoint Security. În acest caz, monitorizarea are efect numai pentru modulele DLL și driverele încărcate în timp ce se execută Kaspersky Endpoint Security.

Atunci când monitorizezi module DLL și drivere, nu este recomandabil să utilizezi reguli Control pornire aplicații create pe baza categoriilor KL. Este posibil ca determinarea categoriilor KL (inclusiv din regulile „Sistemul de operare și componentele sale”) pentru module DLL și drivere să nu funcționeze corect. În particular, regula „Sistemul de operare și componentele sale” a fost creată în mod implicit și nu este distribuită la lansarea modulelor DLL și driverelor. Atunci când activezi această funcție, este necesar să creezi reguli de permitere separate pentru module DLL și drivere. Utilizarea funcției **Control module DLL și drivere** dacă nu există astfel de reguli de permitere poate cauza instabilitatea sistemului.

Îți recomandăm să activezi protecția prin parolă pentru a configura setări pentru program astfel încât să poți dezactiva regulile de permitere care blochează lansarea modulelor DLL și driverelor de importanță critică fără a modifica setări ale politicii Kaspersky Security Center.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Administrarea regulilor pentru Control la pornirea aplicației folosind Kaspersky Security Center

Această secțiune conține informații despre utilizarea Kaspersky Security Center pentru a configura regulile pentru Control la pornirea aplicației și oferă recomandări pentru utilizarea optimă a componentei Control pornire aplicații.

## Colectarea informațiilor despre aplicațiile instalate pe computerele utilizatorilor

Pentru a crea reguli optime pentru Control la pornirea aplicației, se recomandă mai întâi să analizezi aplicațiile folosite pe computerele din rețeaua locală. Pentru aceasta poți obține următoarele informații:

- Vanzători, versiuni și localizări ale aplicațiilor folosite în rețeaua LAN a companiei.
- Frecvența actualizărilor aplicației.
- Politicile de utilizare a aplicației adoptate în companie (acestea pot fi politici de securitate sau politici administrative).
- Locația de stocare pentru pachetele de distribuție a aplicației.

Informații despre aplicațiile folosite pe computerele din rețeaua LAN a companiei sunt disponibile în directorul **Registrul aplicațiilor** și în directorul **Fișiere executabile**. Directoarele **Registrul aplicațiilor** și **Fișiere executabile** sunt amplasate în directorul **Gestionare aplicație** din nodul Consolă de administrare al Kaspersky Security Center.

Directorul **Registrul aplicațiilor** conține lista de aplicații care au fost detectate de [Agentul de rețea ?](#) instalat pe computerul client.

Directorul **Fișiere executabile** conține o listă cu toate fișierele executabile care au fost lansate vreodată pe computerele client sau care au fost detectate în cursul [activității de inventar a Kaspersky Endpoint Security](#).



Pentru a vizualiza informații generale despre aplicație și despre fișierele sale executabile, precum și despre lista de computere pe care este instalată o aplicație, deschide fereastra de proprietăți pentru o aplicație selectată în directorul **registru Aplicații** sau în directorul **Fișiere executabile**.

## Crearea categoriilor de aplicații

Pentru simplificarea creării regulilor, poți crea categorii de aplicații și le poți folosi atunci când creezi reguli pentru Control la pornirea aplicației.

Se recomandă crearea unei categorii „Aplicații pentru serviciu”, care acoperă setul standard de aplicații care sunt folosite în companie. Dacă diferite grupuri de utilizatori folosesc diferite seturi de aplicații la locul lor de muncă, se poate crea o categorie separată de aplicații pentru fiecare grup de utilizatori.

*Pentru a crea o categorie de aplicații:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectează directorul **Suplimentar** → **Gestionare aplicație** → **Categorii aplicații**.
3. Fă clic pe butonul **Creează o categorie** din spațiul de lucru.  
Pornește expertul de creare a categoriilor de utilizatori.
4. Urmează instrucțiunile din Expertul pentru crearea categoriilor de utilizatori.

## Crearea regulilor pentru Control la pornirea aplicației folosind Kaspersky Security Center

*Pentru a crea o regulă Control la pornirea aplicației folosind Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.

- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.

7. Fă clic pe butonul **Adăugare**.

Se deschide fereastra **Regulă Control la pornirea aplicației**.

8. În lista verticală **Categorie**, selectează categoria de aplicații creată pe baza căreia dorești să creezi o regulă.

9. Specifică lista de utilizatori și/sau grupuri de utilizatori pentru care dorești să configurezi permisiunea de pornire a aplicațiilor din categoria selectată. Pentru aceasta, în tabelul **Coordonatori și drepturile acestora**, fă clic pe butonul **Adăugare**.

Se deschide fereastra Microsoft Windows standard **Select Users or Groups** (Selectare utilizatori și grupuri). Această fereastră permite selectarea utilizatorilor și/sau a grupurilor de utilizatori.

10. În tabelul **Coordonatori și drepturile acestora**:

- Dacă dorești să permiți utilizatorilor și/sau grupurilor de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifează casetele de selectare **Permitere** lângă utilizatorii respectivi.
- Dacă dorești să blochezi utilizatori și/sau grupuri de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifează casetele de selectare **Blocare** lângă utilizatorii respectivi.

11. Bifează caseta de selectare **Refuză pentru alți utilizatori** dacă dorești ca toți utilizatorii care nu apar în coloana **Coordonator** și care nu fac parte din grupul de utilizatori specificat în coloana **Coordonator** să nu poată porni aplicațiile care aparțin categoriei selectate.

12. Dacă dorești ca aplicația Kaspersky Endpoint Security să considere aplicațiile din categoria specificată în regulă drept programe de actualizare de încredere, care au dreptul de a porni alte aplicații pentru care nu sunt definite reguli pentru componenta Control pornire aplicații, bifează caseta de selectare **Programe de actualizare de încredere**.

13. Fă clic pe **OK**.

14. În secțiunea **Control pornire aplicații** a ferestrei de proprietăți ale politicii, fă clic pe butonul **Aplicare**.

## Modificarea stării unei reguli a componentei Control pornire aplicații folosind Kaspersky Security Center

*Pentru a modifica starea unei reguli a componentei Control pornire aplicații:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Control endpoint**, selectează subsecțiunea **Control pornire aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control pornire aplicații.
7. Selectează regula componentei Control pornire aplicații a cărei stare dorești să o modifice.
8. În coloana **Stare**, procedează astfel:
  - Dacă dorești să activezi utilizarea unei reguli, bifează caseta de selectare de lângă regulă.
  - Dacă dorești să dezactivezi utilizarea unei reguli, debifează caseta de selectare de lângă regulă.
9. Fă clic pe butonul **Aplicare**.

## Componenta Control privilegii aplicații

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](https://support.kaspersky.com/KESWin/10SP2/ro-RO/all-in-one.htm).

Această secțiune conține informații despre componenta Control privilegii aplicații și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre Control privilegii aplicații

Control privilegii aplicații împiedică aplicațiile să execute acțiuni care ar putea fi periculoase pentru sistemul de operare și asigură controlul accesului la resursele sistemului de operare și la datele de identitate.

Această componentă controlează activitatea aplicațiilor, inclusiv accesul lor la resursele protejate (cum ar fi fișiere și directoare, chei de registru), utilizând *reguli de control pentru aplicații*. Regulile de control pentru aplicații sunt un set de restricții care se aplică diferitelor acțiuni ale aplicațiilor în sistemul de operare și drepturilor de acces la resursele computerului.

Activitatea de rețea a aplicațiilor este monitorizată de componenta Firewall.

Atunci când o aplicație pornește pentru prima dată, componenta Control privilegii aplicații scanează aplicația și o plasează într-un grup de încredere. Un grup de încredere definește regulile de control pentru aplicații pe care Kaspersky Endpoint Security le aplică atunci când controlează activitatea aplicației.

Îți recomandăm să [participi în Kaspersky Security Network](#) pentru a ajuta la o funcționare mai eficientă a componentei Control drepturi aplicații. Datele obținute prin Kaspersky Security Network îți permit să sortezi aplicațiile în grupuri cu mai multă acuratețe și să aplici reguli optime de control pentru aplicații.

La următoarea pornire a aplicației, Control privilegii aplicații verifică integritatea aplicației. Dacă aplicația nu s-a modificat, componenta îi aplică regulile curente de control pentru aplicații. Dacă aplicația s-a modificat, Control privilegii aplicații o rescanează ca și cum ar fi fost pornită pentru prima dată.

## Limitările controlului pentru dispozitive audio și video

### Despre protecția redării în flux audio

Următoarele lucruri trebuie avute în vedere pentru protecția redării în flux audio:

- Componenta Control drepturi aplicații trebuie să fie activată pentru ca această funcționalitate să funcționeze.
- Dacă aplicația a început să primească fluxul audio înainte de pornirea componentei Control drepturi aplicații, Kaspersky Endpoint Security permite aplicației să primească fluxul audio și nu afișează notificări.
- Dacă ai mutat aplicația în grupul **Nu este de încredere** sau **Restricționat la nivel superior** după ce aplicația a început să primească fluxul audio, Kaspersky Endpoint Security permite aplicației

să primească fluxul audio și nu afișează notificări.

- După modificarea setărilor de acces al aplicației la dispozitivele de înregistrare a sunetului (de exemplu, dacă a fost blocată primirea fluxului audio de către aplicație în fereastra cu setările componentei Control aplicație), această aplicație trebuie repornită pentru a nu mai primi fluxul audio.
- Controlul accesului la fluxul audio de la dispozitivele de înregistrare a sunetului nu depinde de setările de acces la camera Web ale unei aplicații.
- Kaspersky Endpoint Security protejează accesul doar la microfoanele încorporate și la microfoanele externe. Nu sunt acceptate alte dispozitive de redare în flux.
- Kaspersky Endpoint Security nu poate garanta protecția unui flux audio de la dispozitive precum camere DSLR, camere video portabile și camere de acțiune.

## Considerații speciale pentru operarea dispozitivelor audio și video în cursul instalării și upgrade-ului Kaspersky Endpoint Security

Atunci când execuți aplicații de înregistrare sau redare audio și video pentru prima dată după instalarea Kaspersky Endpoint Security, este posibil ca redarea sau înregistrarea audio și video să fie întreruptă. Acest lucru este necesar pentru a activa funcționalitatea care controlează accesul aplicațiilor la dispozitivele de înregistrare a sunetului. Serviciul de sistem care controlează componentele hardware audio va fi repornit atunci când Kaspersky Endpoint Security este executat pentru prima dată.

## Despre accesul aplicațiilor la camerele Web

Funcția de protecție a accesului la camera Web prezintă următoarele considerații și limitări:

- Aplicația controlează numai imaginile video și imaginile statice provenite din procesarea datelor de la camera Web.
- Aplicația controlează fluxul audio dacă acesta face parte din fluxul video primit de la camera Web.
- Aplicația controlează numai camerele Web conectate prin USB sau IEEE1394 și care sunt afișate ca **Dispozitive de imagini** în Manager dispozitive Windows.

## Camere Web acceptate

Kaspersky Endpoint Security acceptă următoarele camere Web:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky nu poate garanta asistență pentru camerele Web care nu sunt specificate în această listă.

## Activarea și dezactivarea componentei Control privilegii aplicații

În mod implicit, componenta Control privilegii aplicații este activată, executându-se în modul recomandat de experții de la Kaspersky. Dacă este necesar, poți dezactiva componenta Control privilegii aplicații.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Control privilegii aplicații în fila Protecție și control din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Control endpoint**.



Se deschide secțiunea **Control endpoint**.

4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Control privilegii aplicații.



Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.

5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa componenta Control privilegii aplicații, selectează **Pornire**.

Pictograma de stare a componentei , care se afișează în stânga liniei Control drepturi aplicații, se transformă în pictograma .

- Pentru a dezactiva componenta Control drepturi aplicații, selectează **Oprire**.

Pictograma de stare a componentei , care se afișează în stânga liniei Control drepturi aplicații, se transformă în pictograma .

*Pentru a activa sau a dezactiva componenta Control privilegii aplicații din fereastra cu setările aplicației:*

1. Deschide fereastra cu setările aplicației.
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. În partea dreaptă a ferestrei, efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Control drepturi aplicații, bifează caseta de selectare **Activare Control drepturi aplicații**.
  - Pentru a dezactiva componenta Control drepturi aplicații, debifează caseta de selectare **Activare Control drepturi aplicații**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Administrarea grupurilor de încredere pentru aplicații

Atunci când o aplicație este pornită pentru prima dată, componenta Control drepturi aplicații verifică securitatea aplicației și o plasează într-un [grup de încredere ?](#).

În prima etapă a scanării aplicației, Kaspersky Endpoint Security caută în baza de date internă de aplicații cunoscute o intrare corespunzătoare și simultan trimite o solicitare către baza de date [Kaspersky Security Network](#) (dacă este disponibilă o conexiune la Internet). Pe baza rezultatelor căutării în baza de date internă și în baza de date Kaspersky Security Network, aplicația este plasată într-un grup de încredere. De fiecare dată când aplicația este pornită, Kaspersky Endpoint Security trimite o solicitare nouă către baza de date KSN și plasează aplicația într-un grup de încredere diferit, dacă reputația aplicației în bazele de date KSN s-a modificat.

Poți selecta un grup de încredere căruia Kaspersky Endpoint Security să-i atribuie automat toate aplicațiile necunoscute. Aplicațiile care au fost pornite înainte de Kaspersky Endpoint Security sunt mutate automat în grupul de încredere specificat în fereastra [Selectare grup de încredere](#).

Componenta controlează doar activitatea de rețea a aplicațiilor lansate înainte de Kaspersky Endpoint Security pe baza regulilor de rețea stabilite în setările Firewall.

## Configurarea setărilor pentru alocarea aplicațiilor în grupuri de încredere

Dacă participarea la Kaspersky Security Network este activată, Kaspersky Endpoint Security trimite către KSN o interogare despre reputația unei aplicații de fiecare dată când aplicația este pornită. Pe baza răspunsului de la KSN, aplicația poate fi mutată într-un grup de încredere diferit de cel specificat în setările componentei Control drepturi aplicații.

*Pentru configurarea setărilor pentru introducerea aplicațiilor în grupuri de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Dacă dorești ca aplicațiile semnate digital de la un vânzător de încredere să fie introduse automat în grupul De încredere, bifează caseta de selectare **Încredere în aplicații cu semnătură digitală**.

*Producătorii de încredere* sunt acei producători de software incluși de Kaspersky în grupul de încredere. De asemenea, puteți [adăuga manual certificatul producătorului în depozitul de certificate de sistem de încredere](#).

4. Alege modul în care aplicațiile necunoscute vor fi introduse în grupuri de încredere:
  - Dacă dorești să utilizezi analiza euristică pentru introducerea aplicațiilor necunoscute în grupuri de încredere, selectează opțiunea **Utilizare analiză euristică pentru definire grup** și specifică în câmpul **Durată maximă pentru definirea grupului** durata de timp alocată scanării aplicațiilor pornite.
  - Dacă dorești să introduci toate aplicațiile necunoscute într-un grup de încredere specificat, selectează opțiunea **Mutare automată în grupul** și selectează grupul de încredere potrivit din lista verticală.



Din motive de securitate, grupul **De încredere** nu este inclus în valorile setării **Mutare automată în grupul**.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea unui grup de încredere

La prima pornire a unei aplicații, Kaspersky Endpoint Security o plasează automat într-un grup de încredere. Dacă este necesar, poți muta manual aplicația în alt grup de încredere.

Specialiștii de la Kaspersky nu recomandă mutarea de aplicații din grupul de încredere atribuit în alt grup de încredere. În schimb, poți edita regulile pentru o aplicație individuală.

*Pentru a schimba grupul de încredere la care a fost atribuită automat o aplicație de către Kaspersky Endpoint Security la prima sa pornire:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Fă clic pe butonul **Aplicații**.  
Se deschide fila **Reguli de control al aplicațiilor** din fereastra **Aplicații**.
4. Selectează aplicația relevantă în fila **Reguli de control al aplicațiilor**.
5. Efectuează una dintre următoarele acțiuni:
  - Fă clic dreapta pentru a afișa meniul contextual al aplicației. În meniul contextual al aplicației, selectează **Mutare în grup <nume grup>**.
  - Pentru a deschide meniul contextual, fă clic pe linkul **De încredere/Restricționat la nivel inferior/Restricționat la nivel superior/Nu este de încredere**. În meniul contextual, selectează grupul de încredere necesar.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Selectarea unui grup de încredere pentru aplicații lansate înainte de Kaspersky Endpoint Security

Componenta controlează doar activitatea de rețea a aplicațiilor pornite înainte de Kaspersky Endpoint Security. Controlul se realizează conform regulilor de rețea specificate în [Setări Firewall](#). Pentru a preciza ce reguli de rețea trebuie aplicate monitorizării activității de rețea pentru aceste aplicații, trebuie să selectezi un grup de încredere.

*Pentru a selecta un grup de încredere pentru aplicații lansate înainte de Kaspersky Endpoint Security:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Fă clic pe butonul **Editare**.  
Aceasta deschide fereastra **Selectare grup de încredere**.
4. Selectează grupul de încredere necesar.
5. Fă clic pe **OK**.
6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Gestionarea regulilor de Control aplicații

În mod implicit, activitatea aplicațiilor este controlată de reguli de control pentru aplicații definite pentru grupul de încredere la care Kaspersky Endpoint Security a atribuit aplicația la prima sa lansare. Dacă este necesar, poți edita regulile de control pentru aplicații pentru un întreg grup de încredere, pentru o aplicație individuală sau pentru un grup de aplicații dintr-un grup de încredere.

Regulile de control pentru aplicații definite pentru aplicații individuale sau pentru grupuri de aplicații dintr-un grup de încredere au prioritate mai mare decât regulile de control pentru aplicații definite pentru un grup de încredere. Cu alte cuvinte, dacă setările pentru regulile de control pentru aplicații pentru o aplicație individuală sau pentru un grup de aplicații dintr-un grup de încredere diferă de setările pentru regulile de control pentru aplicații pentru grupul de încredere, componenta Control privilegii aplicații controlează activitatea aplicației sau a grupului de aplicații din grupul de încredere în conformitate cu regulile de control pentru aplicații aferente aplicației sau grupului de aplicații.

# Modificarea regulilor de control al aplicațiilor pentru grupurile de încredere și pentru grupurile de aplicații

În mod implicit, se creează regulile optime de control pentru aplicații pentru diferitele grupuri de încredere. Setările pentru regulile de control pentru grupuri de aplicații moștenesc valorile setărilor pentru regulile de control pentru grupurile de încredere. Poți edita regulile prestabilite de control pentru grupuri de încredere și regulile de control pentru grupuri de aplicații.

*Pentru a edita reguli de control pentru grupuri de încredere sau reguli de control pentru grupuri de aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. Fă clic pe butonul **Aplicații**.

Această acțiune deschide fila **Reguli de control al aplicațiilor** din fereastra **Control drepturi aplicații**.

4. Selectează grupul de încredere sau grupul de aplicații dorit.

5. În meniul contextual al unui grup de încredere sau al unui grup de aplicații, selectează **Reguli de grup**.

Se deschide fereastra **Reguli pentru control grup de aplicații**.

6. În fereastra **Reguli de control pentru grupuri de aplicații**, efectuează una dintre următoarele acțiuni:

- Pentru a edita reguli de control pentru grupuri de încredere sau grupuri de aplicații care gestionează drepturile grupului de încredere sau ale grupului de aplicații de a accesa registrul sistemului de operare, fișierele utilizatorilor și setările aplicației, selectează fila **Fișiere și registru de sistem**.
- Pentru a edita reguli de control pentru grupuri de încredere sau grupuri de aplicații care gestionează drepturile grupului de încredere sau ale grupului de aplicații de a accesa procese și obiecte ale sistemului de operare, selectează fila **Drepturi**.

7. Pentru resursa necesară din coloana acțiunii corespunzătoare, fă clic dreapta pentru a se deschide meniul contextual.

8. În meniul contextual, selectează elementul necesar.

- **Moștenire**
- **Permitere**
- **Blocare**
- **Înregistrare evenimente în jurnal**

Dacă editezi reguli de control pentru grupuri de încredere, elementul **Moștenire** nu este disponibil.

9. Fă clic pe **OK**.

10. În fereastra **Aplicații**, fă clic pe **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Editarea unei reguli de control al aplicației

În mod implicit, setările pentru regulile de control pentru aplicații care aparțin unui grup de aplicații sau unui grup de încredere moștenesc valorile setărilor pentru regulile de control pentru grupurile de încredere. Poți edita setările regulilor de control pentru aplicații.

*Pentru a modifica o regulă de control pentru aplicații:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. Fă clic pe butonul **Aplicații**.

Această acțiune deschide fila **Reguli de control al aplicațiilor** din fereastra **Control drepturi aplicații**.

4. Selectează aplicația necesară.

5. Efectuează una dintre următoarele acțiuni:

- În meniul contextual al aplicației, selectează **Reguli de aplicații**.
- Fă clic pe butonul **Suplimentar** din colțul din dreapta-jos al filei **Reguli de control al aplicațiilor**.

Se deschide fereastra **Reguli de control al aplicațiilor**.

6. În fereastra **Reguli de control al aplicațiilor**, efectuează una dintre următoarele acțiuni:

- Pentru a edita reguli de control pentru aplicații care gestionează drepturile aplicației de a accesa registrul sistemului de operare, fișierele utilizatorilor și setările aplicațiilor, selectează fila **Fișiere și registru de sistem**.
- Pentru a edita regulile de control al aplicațiilor care gestionează drepturile aplicației de a accesa procese și obiecte ale sistemului de operare, selectează fila **Drepturi**.

7. Pentru resursa necesară din coloana acțiunii corespunzătoare, fă clic dreapta pentru a se deschide meniul contextual.

8. În meniul contextual, selectează elementul necesar.

- **Moștenire**
- **Permitere**
- **Blocare**
- **Înregistrare evenimente în jurnal**

9. Fă clic pe **OK**.

10. În fereastra **Aplicații**, fă clic pe **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Dezactivarea descărcărilor și a actualizărilor pentru regulile de control al aplicațiilor din baza de date Kaspersky Security Network

În mod implicit, atunci când sunt detectate informații noi despre o aplicație în baza de date Kaspersky Security Network, Kaspersky Endpoint Security aplică regulile de control descărcate din baza de date KSN pentru această aplicație. Apoi poți edita manual regulile de control pentru aplicație.

Dacă, la prima pornire, o aplicație nu se regăsește în baza de date Kaspersky Security Network, însă ulterior se adaugă informații despre această aplicație în baza de date, Kaspersky Endpoint Security actualizează automat, în mod implicit, regulile de control pentru această aplicație.

Poți dezactiva descărcarea regulilor de control pentru aplicații din baza de date Kaspersky Security Network și a actualizărilor automate a regulilor de control pentru aplicațiile necunoscute anterior.

*Pentru a dezactiva descărcarea regulilor de control pentru aplicații din baza de date Kaspersky Security Network și a actualizărilor automate a acestor reguli:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Debifează caseta de selectare **Actualizare reguli de control pentru aplicații necunoscute anterior din bazele de date KSN**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Dezactivarea moștenirii de restricții din procesul părinte

Pornirea unei aplicații poate fi moștenită de utilizator sau de altă aplicație în curs de executare. Atunci când pornirea aplicației este inițiată de altă aplicație, se creează o secvență de pornire, care implică un proces părinte și un proces subordonat.

Atunci când o aplicație încearcă să obțină acces la o resursă protejată, componenta Control privilegii aplicații analizează toate procesele părinte ale acestei aplicații, pentru a stabili dacă aceste procese au drepturile necesare pentru a accesa resursa protejată. Apoi se ține cont de regula de prioritate minimă: atunci când se compară drepturile de acces ale aplicației cu cele ale procesului părinte, pentru activitatea aplicației se aplică drepturile de acces cu prioritate minimă.

Prioritățile drepturilor de acces sunt următoarele:

1. **Permitere** Acest drept de acces are prioritate maximă.
2. **Blocare** Acest drept de acces are prioritate minimă.

Acest mecanism previne utilizarea de către aplicațiile care nu sunt de încredere sau a aplicațiilor cu drepturi restricționate să efectueze acțiuni care necesită anumite privilegii.

Dacă activitatea unei aplicații este blocată datorită lipsei de drepturi acordate unui proces părinte, poți edita aceste drepturi sau dezactiva moștenirea restricțiilor de la procesul părinte.

*Pentru a dezactiva moștenirea de restricții din procesul părinte:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. Fă clic pe butonul **Aplicații**.

Această acțiune deschide fila **Reguli de control al aplicațiilor** din fereastra **Control drepturi aplicații**.

4. Selectează aplicația necesară.

5. În meniul contextual al aplicației, selectează **Reguli de aplicații**.

Se deschide fereastra **Reguli de control al aplicațiilor**.

6. În fereastra **Reguli de control al aplicațiilor**, selectează fila **Excluderi**.

7. Bifează caseta de selectare **Nu moșteni restricții de la procesul părinte (aplicație)**.

8. Fă clic pe **OK**.

9. În fereastra **Aplicații**, fă clic pe **OK**.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Excluderea acțiunilor anumitor aplicații de la regulile de control pentru aplicații

*Pentru a exclude acțiunile anumitor aplicații de la regulile de control pentru aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. Fă clic pe butonul **Aplicații**.

Această acțiune deschide fila **Reguli de control al aplicațiilor** din fereastra **Control drepturi aplicații**.

4. Selectează aplicația necesară.

5. În meniul contextual al aplicației, selectează **Reguli de aplicații**.

Se deschide fereastra **Reguli de control al aplicațiilor**.

6. Selectează fila **Excluderi**.

7. Bifează casetele de selectare de lângă aplicațiile care nu trebuie să fie monitorizate.

8. Fă clic pe **OK**.

9. În fereastra **Aplicații**, fă clic pe **OK**.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Eliminarea regulilor de control al aplicațiilor învechite

În mod implicit, regulile de control pentru aplicațiile care nu au fost pornite în ultimele 60 de zile sunt șterse automat. Poți să modifice durata de păstrare a regulilor de control pentru aplicațiile neutilizate sau să dezactivezi ștergerea automată a acestor reguli.

*Pentru a șterge regulile de control al aplicațiilor învechite:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să șteargă regulile de control pentru aplicațiile neutilizate, bifează caseta de selectare **Ștergere reguli pentru aplicațiile care nu sunt pornite mai mult de** și specifică numărul relevant de zile.
  - Pentru a dezactiva ștergerea automată a regulilor de control pentru aplicațiile neutilizate, debifează caseta de selectare **Ștergere reguli pentru aplicațiile care nu sunt pornite mai mult de**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Protejarea resurselor sistemului de operare și a datelor de identitate

Componenta Control privilegii aplicații gestionează drepturile aplicației de a efectua acțiuni asupra unor diverse categorii de resurse de sistem și de date de identitate.

Specialiștii de la Kaspersky au elaborat categorii prestabilite de resurse protejate. Categoriile de resurse protejate și resursele protejate din aceste categorii nu pot fi editate sau șterse.

Se pot efectua următoarele acțiuni:

- Adăugarea unei categorii noi de resurse protejate.
- Adăugarea unei resurse protejate noi.



- Dezactivarea protecției unei resurse.

## Adăugarea unei categorii de resurse protejate

*Pentru a adăuga o categorie nouă de resurse protejate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.  
În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.
3. Fă clic pe butonul **Resurse**.  
Această acțiune deschide eticheta **Resurse protejate** din fereastra **Control drepturi aplicații**.
4. În partea stângă din fila **Resurse protejate**, selectează o categorie de resurse protejate la care dorești să adaugi o categorie nouă de resurse protejate.
5. Fă clic pe butonul **Adăugare** și, în lista verticală, selectează **Categorie**.  
Se deschide fereastra **Categorie de resurse protejate**.
6. În fereastra **Categorie de resurse protejate** care se deschide, introdu un nume pentru noua categorie de resurse protejate.
7. Fă clic pe **OK**.  
Apare un element nou în lista de resurse protejate.
8. În fereastra **Control drepturi aplicații**, fă clic pe **OK**.
9. Pentru a salva modificările, fă clic pe butonul **Salvare**.

După ce adaugi o categorie de resurse protejate, o poți edita sau elimina făcând clic pe butonul **Editare** sau **Eliminare** în partea stânga sus a filei **Resurse protejate**.

## Adăugarea unei resurse protejate

*Pentru a adăuga o resursă protejată:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. Fă clic pe butonul **Resurse**.

Această acțiune deschide eticheta **Resurse protejate** din fereastra **Control drepturi aplicații**.

4. În partea stângă din fila **Resurse protejate**, selectează o categorie de resurse protejate la care dorești să adaugi o nouă resursă protejată.

5. Fă clic pe butonul **Adăugare** și, în lista verticală, selectează tipul de resursă pe care dorești s-o adaugi:

- **Fișier sau director.**
- **Cheie de registru.**

Se deschide fereastra **Resursă protejată**.

6. În fereastra **Resursă protejată**, introdu numele resursei protejate în câmpul **Nume**.

7. Fă clic pe butonul **Răsfoire**.

8. În fereastra care se deschide, specifică setările necesare, în funcție de tipul de resursă protejată pe care dorești s-o adaugi. Fă clic pe **OK**.

9. În fereastra **Resursă protejată**, fă clic pe **OK**.

Apare un element nou în lista de resurse protejate pentru categoria selectată în fila **Resurse protejate**.

10. În fereastra **Control drepturi aplicații**, fă clic pe **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

După ce adaugi o resursă protejată, o poți edita sau elimina făcând clic pe butonul **Editare** sau **Eliminare** în partea stânga sus a filei **Resurse protejate**.

## Dezactivarea protecției resursei

*Pentru a dezactiva protecția resursei:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control drepturi aplicații**.

În partea dreaptă a ferestrei se afișează setările componentei Control privilegii aplicații.

3. În partea dreaptă a ferestrei, fă clic pe butonul **Resurse**.

Această acțiune deschide eticheta **Resurse protejate** din fereastra **Control drepturi aplicații**.

4. Efectuează una dintre următoarele acțiuni:

- În partea stângă a etichetei, în lista de resurse protejate, selectează resursa pentru care dorești să dezactivezi protecția și debifează caseta de selectare de lângă numele ei.
- Fă clic pe **Excluderi** și procedează astfel:
  - a. În fereastra **Excluderi**, fă clic pe butonul **Adăugare**. În lista verticală, selectează tipul de resursă pe care dorești s-o adaugi în lista de excluderi de la protecție pentru componenta Control drepturi aplicații: **Fișier sau director** sau **Cheie de registru**.  
Se deschide fereastra **Resursă protejată**.
  - b. În fereastra **Resursă protejată**, introdu numele resursei protejate în câmpul **Nume**.
  - c. Fă clic pe butonul **Răsfoire**.
  - d. În fereastra care se deschide, specifică setările necesare, în funcție de tipul de resursă pe care dorești s-o adaugi în lista de excluderi de la protecție pentru componenta Control privilegii aplicații.
  - e. Fă clic pe **OK**.
  - f. În fereastra **Resursă protejată**, fă clic pe **OK**.  
Apare un element nou în lista de resurse excluse de la protecție pentru componenta Control drepturi aplicații.

După adăugarea unei resurse la lista de excluderi de la protecție pentru componenta Control drepturi aplicații, o poți edita sau elimina făcând clic pe butonul **Editare** sau **Eliminare** în partea superioară a ferestrei **Excluderi**.

g. În fereastra **Excluderi**, fă clic pe **OK**.

5. În fereastra **Control drepturi aplicații**, fă clic pe **OK**.

6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Monitor de vulnerabilități

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru.  
Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru servere de fișiere.

Această secțiune conține informații despre Monitorul de vulnerabilități și instrucțiuni despre cum se activează și dezactivează componenta.

## Despre Monitorul de vulnerabilități

Componenta Monitor de vulnerabilități execută o scanare în timp real pentru a detecta vulnerabilități în aplicațiile care se execută pe computerul utilizatorului și care sunt lansate de către utilizator. Atunci când componenta Monitor de vulnerabilități este activată, nu trebuie să pornești activitatea Scanare de vulnerabilități. Această scanare este relevantă atunci când nu a fost efectuată nicio [activitate Scanare de vulnerabilități](#) pentru aplicațiile instalate pe computerul utilizatorului sau când această activitate de scanare a fost efectuată cu mult timp în urmă.

## Activarea și dezactivarea Monitorului de vulnerabilități





Componenta Monitor de vulnerabilități este dezactivată în mod implicit. Dacă este necesar, poți activa componenta Monitor de vulnerabilități.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Monitor de vulnerabilități, în fila Protecție și control din fereastra principală a aplicației:*

1. Deschide [fereastra principală a aplicației](#).
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Control endpoint**.  
Se deschide secțiunea **Control endpoint**.
4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Monitor de vulnerabilități.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:

- Pentru a activa componenta Monitor de vulnerabilități, selectează **Pornire**.  
Pictograma de stare a componentei , care se afișează în stânga liniei **Monitor de vulnerabilități**, se schimbă în pictograma .
- Pentru a dezactiva componenta Monitor de vulnerabilități, selectează **Oprire**.  
Pictograma de stare a componentei , care se afișează în stânga liniei **Monitor de vulnerabilități**, se schimbă în pictograma .

*Pentru a activa sau a dezactiva componenta Monitor de vulnerabilități din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează **Monitor de vulnerabilități**.  
În partea dreaptă a ferestrei se afișează setările componentei Monitor de vulnerabilități.
3. În partea dreaptă a ferestrei, efectuează una dintre următoarele acțiuni:
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să lanseze o scanare de vulnerabilități pentru aplicațiile care se execută pe computerul utilizatorului sau care sunt lansate de către utilizator, bifează caseta de selectare **Activare Monitorizare vulnerabilități**.
  - Dacă nu dorești ca aplicația Kaspersky Endpoint Security să lanseze o scanare de vulnerabilități pentru aplicațiile care se execută pe computerul utilizatorului sau care sunt lansate de către utilizator, debifează caseta de selectare **Activare Monitorizare vulnerabilități**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Componenta Control dispozitive

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre componenta Control dispozitive și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre componenta Control dispozitive

Componenta Control dispozitive asigură securitatea datelor confidențiale, restricționând accesul utilizatorului la dispozitive instalate pe computer sau conectate la acesta, inclusiv:

- Dispozitive de stocare a datelor (unități de hard disk, unități amovibile, unități cu bandă, discuri CD/DVD)
- Instrumente de transfer de date (modemuri, plăci de rețea externe)
- Dispozitive destinate transferului de date pe suporturi fizice (imprimante)
- Magistrale de conectare (denumite simplu „magistrale”), care desemnează interfețele destinate conectării de dispozitive la computere (precum USB, FireWire și infraroșu)

Componenta Control dispozitive gestionează accesul utilizatorului la dispozitive aplicând [reguli de acces la dispozitive](#) (denumite și „reguli de acces”) și *reguli de acces la magistrale de conectare* (denumite și „reguli de acces la magistrale”).

## Activarea și dezactivarea componentei Control dispozitive

Componenta Control dispozitive este activată în mod implicit. Dacă este necesar, poți dezactiva componenta Control dispozitive.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Control dispozitive în fila **Protecție și control** din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Control endpoint**.  
Se deschide secțiunea **Control endpoint**.
4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Control dispozitive.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Control dispozitive, selectează **Pornire** în meniu.

- Pentru a dezactiva componenta Control dispozitive, selectează **Opre** în meniu.

*Pentru a activa sau a dezactiva componenta Control dispozitive din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi componenta Control dispozitive, bifează caseta de selectare **Activare Control dispozitive**.
  - Dacă dorești să dezactivezi componenta Control dispozitive, debifează caseta de selectare **Activare Control dispozitive**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Despre regulile de acces la dispozitive și la magistrale de conectare

O regulă de acces la dispozitive este o combinație de parametri care definesc următoarele funcții ale componentei Control dispozitive:

- Permite a accesării de către utilizatorii selectați și/sau de către grupurile de utilizatori selectate a tipurilor de dispozitive specifice pe durata unor anumite intervale de timp.  
Poți să selectezi un utilizator și/sau un grup de utilizatori și să creezi pentru acesta o planificare a accesului la dispozitive.
- Setare a dreptului de citire a conținutului de pe dispozitive de memorie.
- Setare a dreptului de editare a conținutului de pe dispozitive de memorie.

În mod implicit, regulile de acces se creează pentru toate tipurile de dispozitive din clasificarea componentei Control dispozitive. Aceste reguli acordă tuturor utilizatorilor acces complet și în orice moment la dispozitive dacă accesul la magistralele de conectare ale tipurilor de dispozitive respective este permis.

O regulă de acces la o magistrală de conectare permite sau blochează accesul la magistrala de conectare respectivă.

În mod implicit, se creează reguli care permit accesul la magistrale pentru toate magistralele de conectare prezente în clasificarea componentei Control dispozitive.

Nu poți crea sau șterge reguli de acces la dispozitive sau reguli de acces la magistrale de conectare; poți numai să editezi astfel de reguli.

## Despre dispozitivele de încredere

*Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

Pentru lucrul cu dispozitive de încredere sunt disponibile următoarele acțiuni:

- Adăugare a unui dispozitiv la lista de dispozitive de încredere.
- Modificare a utilizatorului și/sau a grupului de utilizatori căruia i se permite accesul la dispozitivul de încredere.
- Ștergere a unui dispozitiv din lista de dispozitive de încredere.

Dacă ai adăugat un dispozitiv la lista de dispozitive de încredere și ai creat o regulă de acces pentru acest tip de dispozitiv care blochează sau restricționează accesul, Kaspersky Endpoint Security decide dacă acordă sau nu acces la dispozitiv în funcție de prezența sa în lista de dispozitive de încredere. Prezența în lista de dispozitive de încredere are o prioritate mai mare decât o regulă de acces.

## Decizii standard privind accesul la dispozitive

După ce utilizatorul conectează un dispozitiv la computer, Kaspersky Endpoint Security decide dacă permite accesul la dispozitivul respectiv.

Decizii standard privind accesul la dispozitive

Nr.	Condiții inițiale	Pași intermediari de efectuat până la luarea unei decizii privind accesul la dispozitiv			Decizie privind accesul la dispozitiv
		Verificare a prezenței dispozitivului în lista de dispozitive de încredere	Verificare a accesului la dispozitiv în funcție de regula de acces	Verificare a accesului la magistrală în funcție de regula de acces la magistrală	



1	Dispozitivul nu este prezent în clasificarea dispozitivelor a componentei Control dispozitive.	Neinclus în lista de dispozitive de încredere.	Nicio regulă de acces.	Nu face obiectul scanării.	Acces permis.
2	Dispozitivul este de încredere.	Inclus în lista de dispozitive de încredere.	Nu face obiectul scanării.	Nu face obiectul scanării.	Acces permis.
3	Accesul la dispozitiv este permis.	Neinclus în lista de dispozitive de încredere.	Acces permis.	Nu face obiectul scanării.	Acces permis.
4	Accesul la dispozitiv depinde de magistrală.	Neinclus în lista de dispozitive de încredere.	Accesul depinde de magistrală.	Acces permis.	Acces permis.
5	Accesul la dispozitiv depinde de magistrală.	Neinclus în lista de dispozitive de încredere.	Accesul depinde de magistrală.	Acces blocat.	Acces blocat.
6	Accesul la dispozitiv este permis. Nu s-a găsit nicio regulă de acces la magistrală.	Neinclus în lista de dispozitive de încredere.	Acces permis.	Nicio regulă de acces la magistrală.	Acces permis.
7	Accesul la dispozitiv este blocat.	Neinclus în lista de dispozitive de încredere.	Acces blocat.	Nu face obiectul scanării.	Acces blocat.
8	Nu s-a găsit nicio regulă de acces la dispozitiv sau la magistrală.	Neinclus în lista de dispozitive de încredere.	Nicio regulă de acces.	Nicio regulă de acces la magistrală.	Acces permis.

9	Nu există nicio regulă de acces la dispozitiv.	Neinclus în lista de dispozitive de încredere.	Nicio regulă de acces.	Acces permis.	Acces permis.
10	Nu există nicio regulă de acces la dispozitiv.	Neinclus în lista de dispozitive de încredere.	Nicio regulă de acces.	Acces blocat.	Acces blocat.

Poți edita regula de acces la dispozitiv după ce conectezi dispozitivul. Dacă dispozitivul este conectat și regula de acces permite accesul la acesta, însă ulterior editezi regula de acces și blochezi accesul, Kaspersky Endpoint Security blochează accesul la următoarea solicitare a dispozitivului de efectuare a unei operațiuni cu fișiere (vizualizare a arborelui de directoare, citire, scriere). Un dispozitiv fără sistem de fișiere este blocat numai după următoarea conectare a dispozitivului.

Dacă un utilizator al computerului pe care este instalat Kaspersky Endpoint Security trebuie să solicite accesul la un dispozitiv care a fost blocat din greșeală, trimite utilizatorului [instrucțiunile de solicitare acces](#).

## Editarea unei reguli de acces la dispozitive

În funcție de tipul de dispozitiv, poți modifica diverse setări de acces, cum ar fi lista de utilizatori care primesc accesul la dispozitiv, planificarea pentru acces și lista de utilizatori cu acces permis/blocat.

*Pentru a edita o regulă de acces la dispozitive:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, selectează fila **Tipuri de dispozitive**.  
Fila **Tipuri de dispozitive** conține reguli de acces pentru toate dispozitivele incluse în clasificarea din componenta Control dispozitive.
4. Selectează regula de acces pe care dorești să o editezi.
5. Fă clic pe butonul **Editare**. Acest buton este disponibil numai tipurile de dispozitive care au un sistem de fișiere.  
Se deschide fereastra **Configurare regulă de acces la dispozitive**.

În mod implicit, o regulă de acces la dispozitive acordă tuturor utilizatorilor acces permanent la tipul de dispozitive specificat. În lista **Utilizatori și/sau grupuri de utilizatori**, această regulă de acces conține grupul **Toate**. În tabelul **Drepturi ale grupului de utilizatori selectat după planificări ale accesului**, această regulă de acces conține intervalul **Planificare implicită** pentru acces la dispozitive, cu drepturi de a efectua toate tipurile de operațiuni cu dispozitivele.

6. Editează setările pentru regula de acces la dispozitive:

- a. Selectează un utilizator și/sau un grup de utilizatori din lista **Utilizatori și/sau grupuri de utilizatori**.

Pentru a edita lista **Utilizatori și/sau grupuri de utilizatori**, utilizează butoanele **Adăugare**, **Editare** și **Eliminare**.

- b. În tabelul **Drepturi ale grupului de utilizatori selectat după planificări ale accesului**, configurează planificarea accesului la dispozitive pentru utilizatorul și/sau grupul de utilizatori selectat. Pentru aceasta, bifează casetele de selectare de lângă numele de planificări de acces corespunzătoare dispozitivelor pe care dorești să le utilizezi în regula pentru acces la dispozitive care urmează să fie editată.

Pentru a edita lista de planificări de acces la dispozitive, utilizează butoanele **Creare**, **Editare**, **Copiere** și **Eliminare** din tabelul **Drepturi ale grupului de utilizatori selectat după planificări ale accesului**.

- c. Pentru fiecare planificare pentru acces la dispozitive folosită în regula editată, specifică operațiunile permise atunci când se lucrează cu dispozitivele. Pentru aceasta, în tabelul **Drepturi ale grupului de utilizatori selectat după planificări ale accesului**, bifează casetele de selectare din coloanele care conțin numele operațiunilor relevante.

- d. Fă clic pe **OK**.

După ce ai editat setările implicite pentru o regulă de acces la dispozitiv, setarea pentru accesul la tipul de dispozitiv din coloana **Acces** din tabelul din fila **Tipuri de dispozitive** se modifică la valoarea *Restricționare prin reguli*.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Adăugarea rapoartelor la sau excluderea rapoartelor din jurnalul de evenimente

Înregistrarea în jurnal a evenimentelor este disponibilă numai pentru operațiunile cu fișiere pe unități amovibile.

*Pentru a activa sau a dezactiva înregistrarea în jurnal a evenimentelor:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.

În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, selectează fila **Tipuri de dispozitive**.

Fila **Tipuri de dispozitive** conține reguli de acces pentru toate dispozitivele incluse în clasificarea din componenta Control dispozitive.
4. Selectează **Unități amovibile** în tabelul de dispozitive.

Butonul **Înregistrare în jurnal** devine disponibil în partea de sus a tabelului.
5. Fă clic pe butonul **Înregistrare în jurnal**.

Astfel se deschide fereastra **Setări de înregistrare în jurnal**.
6. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi înregistrarea în jurnal pentru operațiunile de ștergere și scriere a fișierelor pe unitățile amovibile, bifează caseta de selectare **Activare înregistrare în jurnal**.

Kaspersky Endpoint Security va salva un eveniment în fișierul jurnal și va trimite un mesaj către serverul de administrare Kaspersky Security Center de câte ori utilizatorul efectuează operațiuni de scriere sau ștergere cu fișiere pe unități amovibile.
  - În caz contrar, debifează caseta de selectare **Activare înregistrare în jurnal**.
7. Specifică operațiunile care vor fi înregistrate în jurnal. Pentru aceasta, folosește una dintre metodele următoare:
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să înregistreze în jurnal toate evenimentele, bifează caseta de selectare **Salvează informații despre toate fișierele**.
  - Dacă dorești ca aplicația Kaspersky Endpoint Security să înregistreze în jurnal numai informațiile despre fișierele cu un anumit format, în secțiunea **Filtru pentru formatele de fișier**, bifează casetele de selectare de lângă formatele de fișiere relevante.
8. Specifică acțiunile utilizatorilor Kaspersky Endpoint Security ce trebuie să fie înregistrate în jurnal ca evenimente. Pentru aceasta:
  - a. În secțiunea **Utilizatori**, fă clic pe butonul **Selectare**.

Se deschide fereastra Microsoft Windows standard **Select Users or Groups** (Selectare utilizatori și grupuri).
  - b. Specifică sau editează lista de utilizatori și/sau grupuri de utilizatori.

Atunci când utilizatorii din secțiunea **Utilizatori** scriu în fișiere amplasate pe unități amovibile sau șterg fișiere de pe unități amovibile, Kaspersky Endpoint Security va salva informații despre aceste operațiuni în jurnalul de evenimente și va trimite un mesaj către serverul de administrare Kaspersky Security Center.

9. În fereastra **Setări de înregistrare în jurnal**, fă clic pe **OK**.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Poți vizualiza evenimente asociate cu fișiere de pe unități amovibile în Consola de administrare Kaspersky Security Center din spațiul de lucru al nodului **Server de administrare** din fila **Evenimente**. Pentru ca evenimentele să fie afișate în jurnalul de evenimente Kaspersky Endpoint Security local, trebuie să bifezi caseta de selectare **S-a efectuat o operație cu fișiere** în [setările de notificare](#) pentru componenta Control dispozitive.

## Adăugarea unei rețele Wi-Fi la lista de încredere

Poți permite utilizatorilor să se conecteze la rețele Wi-Fi pe care le consideri a fi sigure, cum ar fi o rețea Wi-Fi de companie. Pentru aceasta, trebuie să adaugi rețea la lista de rețele Wi-Fi de încredere. Component Control dispozitive va bloca accesul la toate rețelele Wi-Fi, cu excepția celor specificate în lista de încredere.

*Pentru a adăuga o rețea Wi-Fi la lista de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, selectează fila **Tipuri de dispozitive**.  
Fila **Tipuri de dispozitive** conține reguli de acces pentru toate dispozitivele incluse în clasificarea din componenta Control dispozitive.
4. În coloana **Acces** de lângă dispozitivul **Wi-Fi**, fă clic dreapta pentru a deschide meniul contextual.
5. Selectează opțiunea **Blocare cu excepții**.
6. În lista de dispozitive, selectează **Wi-Fi** și fă clic pe butonul **Editare**.  
Această acțiune deschide fereastra **Rețele Wi-Fi de încredere**.
7. Fă clic pe butonul **Adăugare**.  
Această acțiune deschide fereastra **Rețele Wi-Fi de încredere**.

## 8. În fereastra **Rețele Wi-Fi de încredere**:

- În câmpul **Nume rețea**, specifică numele rețelei Wi-Fi pe care dorești s-o adaugi în lista de încredere.
- În lista verticală **Tip autentificare**, selectează tipul de autentificare folosită la conectarea la rețeaua Wi-Fi de încredere.
- În lista verticală **Tip criptare**, selectează tipul de criptare folosită pentru securizarea traficului prin rețeaua Wi-Fi de încredere.
- În câmpul **Comentariu** poți specifica orice informație despre rețeaua Wi-Fi adăugată.

O rețea Wi-Fi este considerată a fi de încredere dacă setările sale corespund tuturor setărilor specificate în regulă.

9. În fereastra **Rețele Wi-Fi de încredere**, fă clic pe **OK**.

10. În fereastra **Rețele Wi-Fi de încredere**, fă clic pe **OK**.

## Editarea unei reguli de acces la magistrale de conectare

*Pentru a edita o regulă de acces la magistrale de conectare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. Selectează fila **Magistrale de conectare**.  
În fila **Magistrale de conectare** se afișează regulile de acces pentru toate magistralele de conectare clasificate în componenta Control dispozitive.
4. Selectează regula pentru magistrala de conectare pe care dorești să o editezi.
5. Modifică valoarea parametrului de acces:
  - Pentru a permite accesul la o magistrală de conectare, fă clic pe coloana **Acces** pentru a deschide meniul contextual și selectează **Permite**.
  - Pentru a bloca accesul la o magistrală de conectare, fă clic pe coloana **Acces** pentru a deschide meniul contextual și selectează **Blocare**.

6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Acțiuni cu dispozitive de încredere

Această secțiune conține informații despre acțiunile cu dispozitive de încredere.

## Adăugarea unui dispozitiv la lista De încredere din interfața aplicației

În mod implicit, atunci când un dispozitiv este adăugat la lista de dispozitive de încredere, accesul la dispozitiv este acordat tuturor utilizatorilor (grupul de utilizatori Toți).

*Pentru a adăuga un dispozitiv la lista De încredere din interfața aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, selectează fila **Dispozitive de încredere**.
4. Fă clic pe butonul **Selectare**.  
Se deschide fereastra **Selectare dispozitive de încredere**.
5. Bifează caseta de selectare de lângă numele dispozitivului pe care dorești să îl adaugi la lista de dispozitive de încredere.  
Lista din coloana **Dispozitive** depinde de valoarea selectată în lista verticală **Afișare dispozitive conectate**.
6. Fă clic pe butonul **Selectare**.  
Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**.
7. În fereastra **Selectare utilizatori și/sau grupuri** din Microsoft Windows, specifică utilizatorii și/sau grupurile de utilizatori pentru care Kaspersky Endpoint Security recunoaște dispozitivele selectate ca fiind de încredere.  
Numele de utilizatori și/sau de grupuri de utilizatori specificate în fereastra **Selectare utilizatori și/sau grupuri de utilizatori** din Microsoft Windows sunt afișate în câmpul **Permitere pentru utilizatorii și/sau grupurile de utilizatori**.
8. În fereastra **Selectare dispozitive de încredere**, fă clic pe **OK**.  
În tabel, în fila **Dispozitive de încredere** a ferestrei cu setările componentei **Control dispozitive**, se afișează o linie care conține parametrii dispozitivului de încredere adăugat.

9. Repetă pașii 4–7 pentru fiecare dispozitiv pe care dorești să-l adaugi la lista de dispozitive de încredere pentru utilizatorii și/sau grupurile de utilizatori specificate.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Adăugarea dispozitivelor la lista De încredere pe baza modelului sau ID-ului dispozitivului

În mod implicit, atunci când un dispozitiv este adăugat la lista de dispozitive de încredere, accesul la dispozitiv este acordat tuturor utilizatorilor (grupul de utilizatori Toți).

*Pentru a adăuga dispozitive la lista De încredere pe baza modelului sau ID-ului dispozitivului:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să creezi o listă de dispozitive de încredere.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.
7. În partea dreaptă a ferestrei, selectează fila **Dispozitive de încredere**.
8. Fă clic pe butonul **Adăugare**.

Se deschide meniul contextual al butonului.
9. În meniul contextual al butonului **Adăugare**, efectuează una dintre următoarele acțiuni:
  - Selectează butonul **Dispozitive după ID** dacă dorești să selectezi dispozitive cu ID-uri unice cunoscute de adăugat în lista de dispozitive de încredere.
  - Selectează elementul **Dispozitive după model** pentru a adăuga la listă dispozitivele de încredere cu VID (ID vânzător) și PID (ID produs) cunoscute.



10. În fereastra care se deschide, în lista verticală **Tip dispozitiv**, selectează tipul de dispozitive de afișat în tabelul de mai jos.
11. Fă clic pe butonul **Reîmprospătare**.

Tabelul afișează o listă de dispozitive pentru care ID-urile și/sau modelele de dispozitiv sunt cunoscute și care aparțin tipului selectat în lista verticală **Tip dispozitiv**.
12. Bifează casetele de selectare de lângă numele dispozitivelor pe care dorești să le adaugi la lista de dispozitive de încredere.
13. Fă clic pe butonul **Selectare**.

Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**.
14. În fereastra **Selectare utilizatori și/sau grupuri** din Microsoft Windows, specifică utilizatorii și/sau grupurile de utilizatori pentru care Kaspersky Endpoint Security recunoaște dispozitivele selectate ca fiind de încredere.

Numele de utilizatori și/sau de grupuri de utilizatori specificate în fereastra **Selectare utilizatori și/sau grupuri de utilizatori** din Microsoft Windows sunt afișate în câmpul **Permitere pentru utilizatorii și/sau grupurile de utilizatori**.
15. Fă clic pe **OK**.

În linii apar parametrii dispozitivelor de încredere care au fost adăugate în tabelul din fila **Dispozitive de încredere**.
16. Fă clic pe **OK** sau pe **Aplicare** pentru a salva modificările.

## Adăugarea dispozitivelor la lista De încredere pe baza măștii de ID-uri dispozitiv

În mod implicit, atunci când un dispozitiv este adăugat la lista de dispozitive de încredere, accesul la dispozitiv este acordat tuturor utilizatorilor (grupul de utilizatori Toți).

Dispozitivele pot fi adăugate la lista De încredere pe baza măștii pentru ID-ul lor, dar numai în Consola de administrare Kaspersky Security Center.

*Pentru a adăuga dispozitive la lista De încredere pe baza măștii pentru ID-ul lor:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să creezi o listă de dispozitive de încredere.

3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.
7. În partea dreaptă a ferestrei, selectează fila **Dispozitive de încredere**.
8. Fă clic pe butonul **Adăugare**.

Se deschide meniul contextual al butonului.
9. În meniul contextual al butonului **Adăugare**, selectează elementul **Dispozitive după masca de ID**.

Se deschide fereastra **Adăugare dispozitive de încredere după masca de ID**.
10. În fereastra **Adăugare dispozitive de încredere după masca de ID**, introdu masca pentru ID-uri de dispozitiv în câmpul **Mască**.
11. Fă clic pe butonul **Selectare**.

Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**.
12. În fereastra **Selectare utilizatori și/sau grupuri** din Microsoft Windows, specifică utilizatorii și/sau grupurile de utilizatori pentru care Kaspersky Endpoint Security recunoaște ca fiind de încredere dispozitivele ale căror modele sau ID-uri corespund măștii specificate.

Numele de utilizatori și/sau de grupuri de utilizatori specificate în fereastra **Selectare utilizatori și/sau grupuri de utilizatori** din Microsoft Windows sunt afișate în câmpul **Permitere pentru utilizatorii și/sau grupurile de utilizatori**.
13. Fă clic pe **OK**.

În tabelul din fila **Dispozitive de încredere** din fereastra de setări pentru componenta **Control dispozitiv**, apare o linie cu setările regulii pentru adăugarea dispozitivelor la lista de dispozitive de încredere după masca de ID-uri.
14. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea accesului utilizatorului la un dispozitiv de încredere

În mod implicit, atunci când un dispozitiv este adăugat la lista de dispozitive de încredere, accesul la dispozitiv este acordat tuturor utilizatorilor (grupul de utilizatori Toți). Poți configura accesul utilizatorilor (sau al grupurilor de utilizatori) la un dispozitiv de încredere.

*Pentru a configura accesul utilizatorului la un dispozitiv de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.  
În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, selectează fila **Dispozitive de încredere**.
4. În lista de dispozitive de încredere, selectează un dispozitiv pentru care dorești să editezi regulile de acces.
5. Fă clic pe butonul **Editare**.  
Se deschide fereastra **Configurare regulă de acces la dispozitive de încredere**.
6. Fă clic pe butonul **Selectare**.  
Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**.
7. În fereastra **Selectare utilizatori și/sau grupuri** din Microsoft Windows, specifică utilizatorii și/sau grupurile de utilizatori pentru care Kaspersky Endpoint Security recunoaște dispozitivele selectate ca fiind de încredere.
8. Fă clic pe **OK**.  
Numele de utilizatori și/sau de grupuri de utilizatori specificate în fereastra **Selectare utilizatori și/sau grupuri de utilizatori** din Microsoft Windows sunt afișate în câmpul **Permitere pentru utilizatorii și/sau grupurile de utilizatori** din fereastra **Configurare regulă de acces la dispozitive de încredere**.
9. Fă clic pe **OK**.
10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Eliminarea unui dispozitiv din lista de dispozitive de încredere

*Pentru a elimina un dispozitiv din lista de dispozitive de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.

În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.

3. În partea dreaptă a ferestrei, selectează fila **Dispozitive de încredere**.
4. Selectează dispozitivul pe care dorești să îl elimini din lista de dispozitive de încredere.
5. Fă clic pe butonul **Eliminare**.
6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Kaspersky Endpoint Security decide asupra accesului la un dispozitiv pe care l-ai eliminat din lista de dispozitive de încredere în funcție de regulile de acces la dispozitive și de regulile de acces la magistralele de conectare.

## Editarea șabloanelor de mesaje ale componentei Control dispozitive

Atunci când utilizatorul încearcă să acceseze un dispozitiv blocat, aplicația Kaspersky Endpoint Security afișează un mesaj în care se specifică faptul că dispozitivul este blocat sau că o operațiune cu conținutul dispozitivului este interzisă. Dacă utilizatorul consideră că accesul la dispozitiv este blocat în mod eronat sau că o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală, utilizatorul poate trimite un mesaj către administratorul rețelei locale a companiei făcând clic pe linkul din mesajul afișat despre acțiunea blocată.

Sunt disponibile șabloane pentru mesaje de reclamație și șabloane pentru mesajele despre accesul blocat la dispozitive sau despre operațiunile interzise cu conținutul dispozitivului și pentru mesajul trimis către administrator. Poți modifica șabloanele de mesaje.

*Pentru a edita șabloanele pentru mesajele componentei Control dispozitive:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control dispozitive**.

În partea dreaptă a ferestrei se afișează setările componentei Control dispozitive.
3. În partea dreaptă a ferestrei, fă clic pe butonul **Șabloane**.

Se deschide fereastra **Șabloane de mesaje**.
4. Efectuează una dintre următoarele acțiuni:
  - Pentru a modifica șablonul mesajului despre accesul blocat la un dispozitiv sau despre o operațiune interzisă cu conținutul dispozitivului, selectează fila **Blocare**.

- Pentru a modifica șablonul mesajului trimis către administratorul rețelei LAN, selectează fila **Mesaj către administrator**.

5. Editează șablonul mesajului. Mai poți folosi următoarele butoane: **Variabilă**, **Implicit** și **Link** (acest buton este disponibil numai în fila **Blocare**).

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Obținerea accesului la un dispozitiv blocat

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.

Funcționalitatea Kaspersky Endpoint Security care acordă acces temporar la un dispozitiv este disponibilă numai atunci când aplicația Kaspersky Endpoint Security funcționează conform politicii Kaspersky Security Center, iar funcționalitatea respectivă este activată în setările de politică (vezi *Ghidul administratorului Kaspersky Security Center*).

*Pentru a solicita accesul la un dispozitiv blocat din fereastra cu setări ale componentei Control dispozitiv:*

1. În fereastra principală a aplicației, selectează fila **Protecție și control**.
2. Fă clic pe secțiunea **Control endpoint**.  
Se deschide secțiunea **Control endpoint**.
3. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Control dispozitive.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
4. Fă clic pe butonul **Acces la dispozitiv**.  
Se deschide fereastra **Solicitare acces la dispozitive**.
5. Din lista de dispozitive conectate selectează-l pe cel la care dorești să obții acces.
6. Fă clic pe butonul **Generare fișier de solicitare acces**.  
Se deschide fereastra **Creare fișier de solicitare acces**.
7. În câmpul **Durată acces**, specifică perioada de timp pentru care dorești să ai acces la dispozitiv.
8. Fă clic pe butonul **Salvare**.

Se deschide fereastra standard **Salvare fișier solicitare acces** din Microsoft Windows.

9. În fereastra **Salvare fișier solicitare acces** din Microsoft Windows, selectează directorul în care dorești să salvezi fișierul de solicitare acces pentru dispozitiv și fă clic pe butonul **Salvare**.

10. Trimite fișierul de solicitare acces la dispozitiv către administratorul rețelei locale.

11. Primește fișierul cu cheia de acces la dispozitiv de la administratorul rețelei locale.

12. În fereastra **Solicitare acces la dispozitive**, fă clic pe butonul **Activare cheie de acces**.

Se deschide fereastra Microsoft Windows standard **Deschidere cheie de acces**.

13. În fereastra Microsoft Windows **Deschidere cheie de acces**, selectează fișierul cu cheia de acces la dispozitiv primit de la administratorul rețelei locale și fă clic pe butonul **Deschidere**.

Se deschide fereastra **Activare cheie de acces pentru dispozitiv**, care afișează informații despre accesul acordat.

14. În fereastra **Activare cheie de acces pentru dispozitiv**, fă clic pe **OK**.

*Pentru a solicita accesul la un dispozitiv blocat făcând clic pe linkul din mesajul care informează că dispozitivul este blocat:*

1. În fereastra mesajului informativ cu privire la faptul că un dispozitiv sau o magistrală de conectare este blocată, fă clic pe linkul **Solicitare acces**.

Se deschide fereastra **Creare fișier de solicitare acces**.

2. În câmpul **Durată acces**, specifică perioada de timp pentru care dorești să ai acces la dispozitiv.

3. Fă clic pe butonul **Salvare**.

Se deschide fereastra standard **Salvare fișier solicitare acces** din Microsoft Windows.

4. În fereastra **Salvare fișier solicitare acces** din Microsoft Windows, selectează directorul în care dorești să salvezi fișierul de solicitare acces pentru dispozitiv și fă clic pe butonul **Salvare**.

5. Trimite fișierul de solicitare acces la dispozitiv către administratorul rețelei locale.

6. Primește fișierul cu cheia de acces la dispozitiv de la administratorul rețelei locale.

7. În fereastra **Solicitare acces la dispozitive**, fă clic pe butonul **Activare cheie de acces**.

Se deschide fereastra Microsoft Windows standard **Deschidere cheie de acces**.

8. În fereastra Microsoft Windows **Deschidere cheie de acces**, selectează fișierul cu cheia de acces la dispozitiv primit de la administratorul rețelei locale și fă clic pe butonul **Deschidere**.

Se deschide fereastra **Activare cheie de acces pentru dispozitiv**, care afișează informații despre accesul acordat.

9. În fereastra **Activare cheie de acces pentru dispozitiv**, fă clic pe **OK**.

Durata în decursul căreia este acordat accesul la dispozitiv poate diferi de durata pe care ai solicitat-o. Accesul la dispozitiv este acordat pentru perioada de timp specificată de administratorul rețelei locale atunci când a generat cheia de acces la dispozitiv.

## Crearea unei chei pentru accesarea unui dispozitiv blocat folosind Kaspersky Security Center

Pentru a acorda unui utilizator acces temporar la un dispozitiv blocat, este necesară o cheie de acces la dispozitiv. Poți crea o cheie de acces folosind Kaspersky Security Center.

*Pentru a crea o cheie de acces pentru un dispozitiv blocat:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În lista de computere client, selectează computer al cărui utilizator trebuie să primească acces temporar la un dispozitiv blocat.
5. În meniul contextual al computerului, selectează opțiunea **Acordă acces la dispozitive și la date în modul offline**.

Se deschide fereastra **Acordă acces la dispozitive și la date în modul offline**.

6. Selectează fila **Control dispozitiv**.

7. În fila **Control dispozitiv**, fă clic pe butonul **Răsfoire**.

Se deschide fereastra Microsoft Windows standard **Selectare fișier solicitare acces**.

8. În fereastra **Selectare fișier solicitare acces**, selectează fișierul de solicitare acces primit de la utilizator și fă clic pe butonul **Deschidere**.

Fila **Control dispozitiv** afișează detaliile dispozitivului blocat la care utilizatorul a solicitat accesul.

9. Specifică valoarea pentru setarea **Durată acces**.

Această setare definește perioada de timp pentru care acorzi utilizatorului acces la dispozitivul blocat. Valoarea implicită este egală cu cea specificată de utilizator la crearea fișierului de solicitare acces.

10. Specifică valoarea pentru setarea **Perioadă de activare**.

Această setare definește perioada de timp pentru care utilizatorul poate activa accesul la dispozitivul blocat folosind cheia de acces furnizată.

11. Fă clic pe butonul **Salvare**.

Se deschide fereastra standard **Salvare cheie de acces** din Microsoft Windows.

12. Selectează directorul de destinație în care dorești să salvezi fișierul care conține cheia de acces pentru dispozitivul blocat.

13. Fă clic pe butonul **Salvare**.

## Componenta Control Web

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune conține informații despre componenta Control Web și instrucțiuni despre configurarea setărilor pentru această componentă.

## Despre componenta Control Web

Componenta Control Web permite controlarea acțiunilor utilizatorilor dintr-o rețea LAN, restricționând sau blocând accesul la resurse Web.

O resursă Web reprezintă o singură pagină Web sau mai multe pagini Web ori un singur site Web sau mai multe site-uri Web care au o particularitate comună.

Componenta Control Web oferă următoarele opțiuni:

- Economisirea traficului.

Traficul este controlat prin restricționarea sau blocarea descărcărilor de fișiere multimedia sau prin restricționarea sau blocarea accesului la resurse Web care nu au legătură cu responsabilitățile profesionale ale utilizatorului.



- Delimitarea accesului în funcție de categoriile de conținut al resurselor Web.

Pentru a economisi traficul și a reduce potențialele pierderi rezultate în urma utilizării necorespunzătoare a orelor de program de către angajați, poți restricționa sau bloca accesul la categoriile de resurse Web specifice (de exemplu, blocarea accesului la resurse Web care fac parte din categoria „Medii comunicații Internet”).

- Controlul centralizat al accesului la resurse Web.

Dacă utilizezi Kaspersky Security Center, sunt disponibile setări personale și de grup pentru acces la resursele Web.

Toate restricțiile și blocările aplicate pentru acces la resurse Web sunt implementate ca [reguli de acces pentru resurse Web](#).

## Activarea și dezactivarea componentei Control Web

Componenta Control Web este activată în mod implicit. Dacă este necesar, poți dezactiva componenta Control Web.

Această componentă poate fi activată sau dezactivată în două moduri:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

*Pentru a activa sau a dezactiva componenta Control Web în fila **Protecție și control** din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Control endpoint**.  
Se deschide secțiunea **Control endpoint**.
4. Fă clic dreapta pentru a afișa meniul contextual al liniei cu informații despre componenta Control Web.  
Se deschide un meniu pentru selectarea de acțiuni de efectuat asupra componentei.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa componenta Control Web, selectează **Pornire** în meniu.
  - Pentru a dezactiva componenta Control Web, selectează **Oprește** în meniu.

*Pentru a activa sau a dezactiva componenta Control Web din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să activezi componenta Control Web, bifează caseta de selectare **Activare Control Web**.
- Dacă dorești să dezactivezi componenta Control Web, debifează caseta de selectare **Activare Control Web**.

În cazul în care componenta Control Web este dezactivată, aplicația Kaspersky Endpoint Security nu controlează accesul la resurse Web.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Categorii de conținut pentru resurse Web

Categoriile de conținut pentru resursele Web (denumite în continuare „categorii”) listate mai jos au fost selectate pentru a descrie cât mai complet blocurile de date găzduite de resurse Web, luând în calcul caracteristicile lor funcționale și tematice. Ordinea în care apar aceste categorii în listă nu reflectă importanța relativă sau prevalența acestor categorii pe Internet. Numele de categorii sunt provizorii și sunt folosite doar pentru produse și site-uri Web ale Kaspersky. Numele nu reflectă în mod obligatoriu semnificația acordată în legislație. O resursă web poate aparține mai multor categorii în același timp.

### Conținut pentru adulți

Această categorie include următoarele tipuri de resurse Web:

- Resurse Web care conțin orice materiale cu fotografii sau clipuri video care descriu organele genitale ale unor oameni sau ale unor creaturi umanoide, acte sexuale sau de auto-stimulare efectuate de oameni sau de creaturi umanoide.
- Resurse Web care conțin orice materiale text, inclusiv materiale artistice sau literare, care descriu organele genitale ale unor oameni sau ale unor creaturi umanoide, acte sexuale sau de auto-stimulare efectuate de oameni sau de creaturi umanoide.
- Resurse Web dedicate discutării aspectului sexual al relațiilor umane.

Se suprapune uneori cu categoria „Medii comunicații Internet”.

- Resurse Web care conțin materiale erotice, lucrări care oferă o descriere realistă a comportamentului sexual la oameni sau lucrări de artă destinate stimulării apetitului sexual.
- Resurse Web ale unor porturi de media oficiale și comunități online cu un public țintă stabilit, care conțin o rubrică specială și/sau articole individuale consacrate aspectului sexual al relațiilor umane.
- Resurse Web consacrate perversiunilor sexuale.
- Resurse Web care fac publicitate și care vând articole care sunt utilizate în sex și pentru stimularea apetitului sexual, servicii sexuale și de întâlniri intime, inclusiv servicii oferite online prin chat-uri video erotice, „sex prin telefon”, „sexting” („sex virtual”).
- Resurse Web cu următorul conținut:
  - Articole și bloguri care tratează educația sexuală prin teme științifice și populare.
  - Enciclopedii medicale, în special secțiunile acestora despre reproducerea sexuală.
  - Resursele instituțiilor medicale, în special secțiunile acestora despre tratamentul organelor sexuale.

## Software, audio, video

Această categorie include următoarele subcategorii pe care le poți selecta individual:

- **Audio și video.**

Această subcategorie include resurse Web care distribuie materiale audio și video: filme, înregistrări ale unor emisiuni sportive, înregistrări de concerte, cântece, clipuri din filme, clipuri video, înregistrări cu tutoriale audio și video etc.

- **Torrente.**

Această subcategorie include site-uri Web cu programe de urmărire pentru torrente, destinate partajării fișierelor cu dimensiune nelimitată.

- **Partajare fișier.**

Această subcategorie include site-uri Web pentru partajarea de fișiere, indiferent de locația fizică a fișierelor care sunt distribuite.

## Alcool, tutun, narcotice

Această subcategorie include site-uri Web al căror conținut este legat direct sau indirect le alcool sau produse care conțin alcool, produse din tutun și narcotice, substanțe psihotropice și/sau intoxicante.

- Resurse Web care fac publicitate și comercializează astfel de substanțe și accesorii pentru consumul acestora.

Se suprapune uneori cu categoria „Comerț electronic”.

- Resurse Web cu instrucțiuni consacrate consumului sau producerii de narcotice, substanțe psihotropice și/sau intoxicante.

Această categorie include resurse Web care abordează subiecte științifice sau de antură medicală.

## Violență

Această categorie include resurse Web care conțin fotografii, clipuri video sau materiale text care descriu acte de violență fizică sau psihologică împotriva unor ființe umane sau tratament inuman împotriva animalelor.

- Resurse Web care descriu scene de execuții, tortură sau abuz, precum și instrumente pentru astfel de practici.

Se suprapune uneori cu categoria „Arme, explozibili, materiale pirotehnice”.

- Resurse Web care descriu scene de crimă, bătăi sau viol, scene în care oameni, animale sau creaturi imaginare sunt abuzate sau umilite.
- Resurse Web cu informații care incită la acțiuni care pun în pericol viața și/sau sănătatea, inclusiv automutilare sau sinucidere.
- Resurse Web cu informații care documentează sau justifică admisibilitatea violenței și/sau a cruzimii sau care incită la acte violente împotriva oamenilor sau a animalelor.
- Resurse Web cu descrieri extrem de realiste ale victimelor și atrocităților războiului, conflictelor armate și confruntărilor militare, accidentelor, catastrofelor, dezastrelor naturale, cataclismelor

industriale sau sociale sau ale suferințelor umane.

- Jocuri de computer în browser cu scene de violență și cruzime, inclusiv așa-numitele jocuri de tip „shooter”, „fightings”, „slashers” etc.

Se suprapune uneori cu categoria „Jocuri de computer”.

## Arme, explozibili, materiale pirotehnice

Această categorie include resurse Web cu informații despre arme, explozibili și produse pirotehnice:

- Site-uri Web ale producătorilor și ale magazinelor de arme, explozibili și produse pirotehnice.

Se suprapune uneori cu categoria „Comerț electronic”.

- Resurse Web consacrate producerii sau folosirii armelor, explozibililor și produselor pirotehnice.
- Resurse Web care conțin materiale analitice, istorice, enciclopedice și materiale care privesc fabricarea armelor, explozibililor și produselor pirotehnice.

Termenul „arme” se referă la aplicații, articole, elemente și mijloace destinate afectării vieții sau sănătății oamenilor și animalelor și/sau producerii de pagube la adresa echipamentelor și structurilor.

## Vulgaritate

Această categorie include resurse Web în care a fost detectat un limbaj vulgar.

Se suprapune uneori cu categoria „Conținut pentru adulți”.

Această categorie mai include resurse Web cu materiale lingvistice și filologice care au ca obiect de studiu vulgaritatea.

## Jocuri de noroc, loterii, pronosport

Această categorie include resurse Web care oferă utilizatorilor posibilitatea de a avea o participare de natură financiară în jocuri de noroc, chiar dacă această participare de natură financiară nu este o condiție obligatorie pentru accesul la site-ul Web respectiv. Această categorie include resurse Web care oferă:

- Jocuri de noroc în care participanților li se solicită să aibă contribuții monetare.

Se suprapune uneori cu categoria „Jocuri de computer”.

- Jocuri de tip pronosport care implică pariuri pe bani.
- Loterii care implică achiziționare de bilete sau numere de loterie.
- Informații care pot declanșa dorința de a participa în jocuri de noroc, loterii și pronosport.

Se suprapune uneori cu categoria „Comerț electronic”.

Această categorie include jocuri care oferă participare gratuită ca mod separat, precum și resurse Web care fac în mod activ publicitate unor alte resurse Web care se încadrează în această categorie.

## Comunicații de rețea

Această categorie include resurse Web care permit utilizatorilor (înregistrați sau nu) să trimită mesaje personale către alți utilizatori ale unor resurse Web relevante sau către alte servicii online și/sau să adaugă conținut (care poate sau nu să fie accesat public) în resurse Web relevante, în anumite condiții. Poți selecta individual următoarele subcategorii:

- **Conversații Web și forumuri.**

Această subcategorie include resurse Web destinate discutării publice a unor diverse subiecte, folosind aplicații Web speciale, precum și resurse Web consacrate distribuirii sau sprijinii aplicațiilor de mesagerie instantanee care permit comunicarea în timp real.

- **Bloguri.**

Această subcategorie include platforme de blog, care sunt site-uri Web ce oferă servicii plătite sau gratuite pentru crearea și întreținerea blogurilor.

- **Rețele sociale.**

Această subcategorie include site-uri Web concepute pentru construirea, afișarea și administrarea contactelor între persoane, organizații și guverne, care necesită înregistrarea unui cont de utilizator drept condiție de participare.

- **Site-uri de întâlniri.**

Această subcategorie include resurse Web care funcționează ca o varietate a rețelelor sociale care oferă servicii plătite sau gratuite.

Se suprapune uneori cu categoriile „Conținut pentru adulți” și „Comerț electronic”.

- **E-mail pe web.**

Această subcategorie include exclusiv pagini de conectare pentru un serviciu de e-mail și pagini de cutii poștale care conțin mesaje de e-mail și date asociate (cum ar fi contacte personale). Această categorie nu include alte pagini Web al unui furnizor de servicii Internet care oferă și servicii de e-mail.

## E-taileri, bănci și sisteme de plată

Această categorie include resurse Web consacrate oricărei tranzacții online ce implică fonduri monetari într-o altă formă decât numerar și care folosesc aplicații Web special construite în acest scop. Poți selecta individual următoarele subcategorii:

- **Magazine și licitații.**

Această subcategorie include magazine și licitații care comercializează orice articole, muncă sau servicii către persoane individuale și/sau către entități legale, inclusiv site-uri Web ale unor magazine care vând exclusiv online și profiluri online ale unor magazine fizice care acceptă plăți online.

- **Bănci.**

Această subcategorie include pagini Web specializate ale băncilor cu funcționalitatea online banking, inclusiv transferuri (electronice) între conturi bancare, realizarea unor depozite în bani, efectuarea unor conversii între devize, plata unor servicii efectuate de terți etc.

- **Sisteme de plată.**

Această subcategorie include pagini Web ale unor sisteme de monede electronice care asigură acces la contul personal al utilizatorului.

În termeni tehnici, plata poate fi efectuată folosind atât carduri bancare de orice tip (plastic sau virtual, debit sau credit, local sau internațional), cât și monede electronice. Resursele Web se pot încadra în această categorie indiferent dacă prezintă sau nu aspecte tehnice precum transmiterea datelor prin protocol SSL, utilizarea autentificării 3D Secure etc.

## Căutare serviciu

Această categorie include resurse Web concepute să-i ajute pe angajatori și pe cei care-și caută serviciu:

- Site-uri Web ale agențiilor de recrutare (agenții de angajare și/sau agenții de headhunting).
- Site-uri Web ale angajatorilor cu descrieri ale locurilor de muncă disponibile și ale avantajelor acestora.
- Portaluri independente cu oferte de angajare de la angajatori și agenții de recrutare.
- Rețele sociale profesionale care, între altele, fac posibilă căutarea sau găsirea informațiilor despre specialiști care nu caută în mod activ un loc de muncă nou.

Se suprapune uneori cu categoria „Medii comunicații Internet”.

## Sisteme de accesare anonime

Această categorie include resurse Web care acționează ca intermediar în descărcarea conținutului altor resurse Web folosind aplicații Web speciale în scopurile următoare:

- Ocolirea restricțiilor impuse de un administrator al unei rețele LAN cu privire la accesul la adrese Web sau adrese IP;
- Accesarea anonimă a resurselor Web, inclusiv resurse Web care resping în mod special solicitările HTTP de la anumite adrese IP sau grupuri de adrese IP (de exemplu, adrese IP grupate după țara de origine).

Această categorie include atât resurse Web destinate exclusiv scopurilor mai sus menționate („instrumente de anonimizare”), cât și resurse Web cu funcționalitate tehnică asemănătoare.



## Jocuri de computer

Această categorie include resurse Web consacrate jocurilor de computer de diferite genuri:

- Site-uri Web ale dezvoltatorilor de jocuri de computer.
- Resurse Web consacrate discuțiilor referitoare la jocuri de computer.

Se suprapune uneori cu categoria „Medii comunicații Internet”.

- Resurse Web care oferă posibilitatea tehnică de a participa online la jocuri de computer, împreună cu alți participanți sau individual, cu instalarea locală a unor aplicații sau fără instalarea locală a unor astfel de aplicații („jocuri în browser”).
- Resurse Web consacrate publicității, distribuției și suportului pentru programe software de gaming.

Se suprapune uneori cu categoria „Comerț electronic”.

## Religii, asociații religioase

Această categorie include resurse Web cu materiale despre mișcări populare, asociații și organizații cu o ideologie religioasă și/sau de cult, indiferent de manifestarea acestora.

- Site-uri web ale unor organizații religioase oficiale, la diferite niveluri, de la organizații internaționale la comunități religioase locale.
- Site-uri Web ale unor asociații și societăți religioase care au apărut ca urmare a separării dintr-o asociație sau comunitate religioasă dominantă.
- Site-uri Web ale unor asociații și comunități religioase care au apărut independent de mișcările religioase tradiționale, inclusiv la inițiativa unui anumit fondator.
- Site-uri Web ale unor organizații interconfesionale care urmăresc cooperarea între reprezentanți ai unor diferite religii tradiționale.
- Resurse Web cu materiale Web educaționale, istorice și enciclopedice care au drept subiect religii.
- Resurse Web cu portretizări detaliate ale actului adorării ca parte a culturilor religioase, inclusiv rituri și ritualuri care implică adorarea lui Dumnezeu, a unor ființe și/sau alte articole considerate

a avea puteri supranaturale.

## Medii știri

Această categorie include resurse Web cu știri publice create de mass media sau de publicații online care permit utilizatorilor să adauge propriile lor știri:

- Site-uri Web ale posturilor oficiale de media.
- Site-uri Web care oferă servicii de informații, cu atribuirea surselor oficiale pentru informații.
- Site-uri Web care oferă servicii de agregare, colecții de informații din știri ,din diverse surse oficiale și neoficiale.
- Site-uri Web în care conținutul știrilor este creat de către utilizatori („site-uri de știri sociale”).

Se suprapune uneori cu categoria „Medii comunicații Internet”.

## Bannere

Această categorie include resurse Web care cu bannere. Informațiile publicitare de pe bannere pot distrage atenția utilizatorilor de la activitățile lor, iar descărcările bannerelor duc la creșterea traficului.

## Despre regulile de acces la resurse Web

O regulă de acces la resurse Web este un set de filtre și acțiuni efectuate de Kaspersky Endpoint Security când utilizatorul vizitează resurse Web descrise în regulă în intervalul de timp indicat în planificarea regulii. Filtrele îți permit să specifice cu precizie un set de resurse Web la care accesul este controlat de componenta Control Web.

Sunt disponibile următoarele filtre:

- **Filtrare după conținut.** Componenta Control Web împarte [resursele Web în categorii în funcție de conținut](#) și tipul datelor. Poți controla accesul utilizatorului la resurse Web cu tipuri de conținut și date din anumite categorii. Când utilizatorii vizitează resurse Web care aparțin categoriei de conținut și/sau categoriei de tip de date selectate, Kaspersky Endpoint Security efectuează acțiunea specificată în regulă.
- **Filtrare după adresele resurselor Web.** Poți controla accesul utilizatorului la toate adresele de resurse Web sau la adrese de resurse Web individuale și/sau la grupuri de adrese de resurse Web.

Dacă sunt specificate filtrarea după conținut și filtrarea după adresele resurselor Web și adresele specificate pentru resurse Web și/sau grupuri de resurse Web aparțin categoriilor de conținut sau categoriilor de tipuri de date selectate, Kaspersky Endpoint Security nu controlează accesul la toate resursele Web din categoriile de conținut și/sau categoriile de tipuri de date selectate. În schimb, aplicația controlează numai accesul la adresele de resurse Web și/sau adresele de grupuri de resurse Web specificate.

- **Filtrare după numele utilizatorilor sau ale grupurilor de utilizatori.** Poți specifica numele utilizatorilor și/sau grupurilor de utilizatori pentru care accesul la resurse Web este controlat după această regulă.
- **Planificare regulă.** Poți specifica planificarea regulii. Planificarea regulii determină intervalul de timp pentru care aplicația Kaspersky Endpoint Security monitorizează accesul la resursele Web la care se aplică regula.

După instalarea Kaspersky Endpoint Security, lista de reguli a componentei Control Web nu este goală. Două reguli sunt presetate:

- Regula Scenarii și tabele de stil, care asigură tuturor utilizatorilor accesul permanent la resursele Web ale căror adrese conțin nume de fișiere cu extensia css, js sau vbs. De exemplu: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- Regula „Default”, care asigură tuturor utilizatorilor accesul la orice resurse Web oricând.

## Acțiuni asupra regulilor de acces la resurse Web

Poți efectua următoarele acțiuni asupra regulilor de acces la resurse Web:

- Adăugare a unei reguli noi
- Editare a unei reguli
- Atribuire a unei priorități unei reguli

Prioritatea unei reguli este definită după poziția liniei care conține o scurtă descriere a acestei reguli în tabelul de reguli de acces din fereastra de setări a componentei Control Web. Aceasta înseamnă că o regulă poziționată mai sus în tabelul de reguli de acces are o prioritate mai mare decât o regulă poziționată sub ea.

Dacă resursa Web pe care utilizatorul încearcă să o acceseze corespunde parametrilor mai multor reguli, Kaspersky Endpoint Security efectuează o acțiune în conformitate cu regula cu prioritatea cea mai mare.

- Testare a unei reguli.

Poți verifica consecvența regulilor utilizând funcția Diagnosticare reguli.

- Activare sau dezactivare a unei reguli.

O regulă de acces pentru o resursă Web poate fi activată (stare de funcționare: *Activat*) sau dezactivată (stare de funcționare: *Dezactivat*). În mod implicit, după ce o regulă este creată, aceasta este activată (stare operațională: *Activat*). Regula poate fi dezactivată.

- Ștergere regulă

## Adăugarea și editarea unei reguli de acces la resurse Web

*Pentru a adăuga sau a edita o regulă de acces la resurse Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. Efectuează una dintre următoarele acțiuni:

- Pentru a adăuga o regulă, fă clic pe butonul **Adăugare**.
- Dacă dorești să editezi o regulă, selectează regula în tabel și apasă pe butonul **Editare**.

Se deschide fereastra **Regulă de acces la resurse Web**.

4. Specifică sau editează setările pentru regulă. Pentru aceasta:

- a. În câmpul **Nume**, introdu sau editează numele regulii.
- b. În lista verticală **Filtrare conținut**, selectează opțiunea necesară:

- **Orice conținut**.
- **După categorii de conținut**.
- **După tipuri de date**.
- **După categorii de conținut și tipuri de date**.

- c. Dacă este selectată o altă opțiune decât **Orice conținut**, se deschid secțiuni pentru selectarea categoriilor de conținut și/sau a tipurilor de date. Bifează casetele de selectare de lângă numele categoriilor de conținut și/sau ale tipurilor de date necesare.

Dacă bifezi caseta de selectare de lângă numele unei categorii de conținut și/sau de tip de date, aplicația Kaspersky Endpoint Security aplică regula de control al accesului resurselor Web care aparțin categoriilor de conținut și/sau tipurilor de date selectate.

d. În lista verticală **Aplicare la adresele**, selectează opțiunea necesară:

- **Pentru toate adresele.**
- **Pentru adresele individuale.**

e. Dacă este selectată opțiunea **Pentru adresele individuale**, se deschide o secțiune în care poți crea o listă de resurse Web. Poți adăuga sau edita lista de resurse Web utilizând butoanele **Adăugare**, **Editare** și **Ștergere**.

f. Bifează caseta de selectare **Specificare utilizatori și/sau grupuri**.

g. Fă clic pe butonul **Selectare**.

Se deschide fereastra Microsoft Windows **Selectare utilizatori și grupuri**.

h. Specifică sau editează lista de utilizatori și/sau grupuri de utilizatori pentru care accesul la resursele Web descrise de regulă urmează să fie permis sau blocat.

i. În lista verticală **Acțiune**, selectează opțiunea necesară:

- **Permitere** Dacă se selectează această valoare, Kaspersky Endpoint Security permite accesul la resurse Web care se potrivesc cu parametrii regulii.
- **Blocare** Dacă se selectează această valoare, Kaspersky Endpoint Security blochează accesul la resurse Web care se potrivesc cu parametrii regulii.
- **Avertizare** Dacă se selectează această valoare, atunci când utilizatorul încearcă să acceseze o resursă Web care corespunde regulii, Kaspersky Endpoint Security afișează o avertizare că resursa Web respectivă nu este recomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

j. În lista verticală **Planificare regulă**, selectează numele planificării necesare sau generează o planificare nouă bazată pe planificarea de regulă selectată. Pentru aceasta:

1. Lângă lista verticală **Planificare regulă**, fă clic pe butonul **Setări**.

Se deschide fereastra **Planificare regulă**.

2. Pentru a adăuga la planificarea regulii un interval de timp în care regula să nu se aplice, în tabelul care afișează planificarea regulii, fă clic pe celulele de tabel care corespund cu ora și ziua din săptămâna pe care dorești să o selectezi.

Culoarea celulelor devine gri.

3. Pentru a înlocui un interval de timp în care regula se aplică cu un interval de timp în care regula nu se aplică, fă clic în tabel pe celulele gri care corespund orei și zilei din săptămâna pe care dorești să o selectezi.

Culoarea celulelor devine verde.

4. Fă clic pe butonul **Salvare ca**.

Se deschide fereastra **Nume planificare regulă**.

5. Tastează un nume pentru planificarea de regulă sau păstrează numele implicit sugerat.

6. Fă clic pe **OK**.

5. În fereastra **Regulă de acces la resurse Web**, fă clic pe **OK**.

6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Atribuirea de priorități regulilor de acces la resurse Web

Poți atribui priorități fiecărei reguli din lista de reguli aranjând regulile într-o anumită ordine.

*Pentru a atribui o prioritate unei reguli de acces la resurse Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Control Web.
3. În partea dreaptă a ferestrei, selectează regula pentru care dorești să schimbi prioritatea.
4. Utilizează butoanele **Mutare sus** și **Mutare jos** pentru a muta regula în poziția dorită din lista de reguli.
5. Repetă pașii 3–4 pentru regulile a căror prioritate dorești s-o schimbi.
6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Testarea regulilor de acces la resurse Web

Pentru a verifica consistența regulilor componentei Control Web, ai posibilitatea să le testezi. În acest scop, componenta Control Web include o funcție Diagnosticare reguli.

*Pentru a testa regulile de acces la resurse Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. În partea dreaptă a ferestrei, fă clic pe butonul **Diagnostiche**.

Se deschide fereastra **Diagnosticare reguli**.

4. Completează câmpurile din secțiunea **Condiții**:

- a. Dacă dorești să testezi regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la o anumită resursă Web, bifează caseta de selectare **Specifică adresa** și introdu adresa resursei Web în câmpul de mai jos.
- b. Dacă dorești să testezi regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la resurse Web pentru anumiți utilizatori și/sau anumite grupuri de utilizatori, specifică o listă de utilizatori și/sau de grupuri de utilizatori.
- c. Dacă dorești să testezi regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la resursele Web cu anumite categorii de conținut și/sau categorii de tipuri de date, în lista verticală **Filtrare conținut**, selectează opțiunea necesară (**După categorii de conținut**, **După tipuri de date** sau **După categorii de conținut și tipuri de date**).
- d. Dacă dorești să testezi regulile luând în considerare ora și ziua din săptămâna în care este efectuată o încercare de accesare a resurselor Web specificate în condițiile pentru diagnostice regulă, bifează caseta de selectare **Includere oră încercare de acces**. Apoi specifică ziua din săptămână și ora.

5. Fă clic pe butonul **Test**.

După finalizarea testării se afișează un mesaj informativ cu privire la acțiunea efectuată de Kaspersky Endpoint Security, în funcție de prima regulă care se declanșează la încercarea de accesare a resurselor Web specificate (permitere, blocare sau avertizare). Prima regulă care se declanșează este cea a cărei poziție în lista de reguli a componentei Control Web este superioară pozițiilor celorlalte reguli care îndeplinesc condițiile de diagnosticare. Mesajul se afișează în dreapta butonul **Test**. Tabloul de mai jos prezintă regulile de declanșare rămase, specificând acțiunea luată de Kaspersky Endpoint Security. Regulile sunt listate în ordine descrescătoare a priorității.

## Activarea și dezactivarea unei reguli de acces la resurse Web

*Pentru a activa sau a dezactiva o regulă de acces la resurse Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. În partea dreaptă a ferestrei, selectează regula pe care dorești să o activezi sau să o dezactivezi.

4. În coloana **Stare**, procedează astfel:

- Dacă dorești să activezi utilizarea regulii, selectează *Activat*.
- Dacă dorești să dezactivezi utilizarea regulii, selectează *Dezactivat*.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Migrarea regulilor de acces la resurse Web de la versiuni anterioare ale aplicației

Atunci când se face upgrade de la Service Pack 1 Maintenance Release 1 sau o versiune anterioară a aplicației la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, regulile de acces la resurse Web bazate pe categorii de conținut pentru resurse Web sunt migrate după cum urmează:

- Regulile de acces la resurse Web bazate pe una sau mai multe categorii de conținut pentru resurse Web din listele „Forumuri și chat-uri”, „E-mail pe Web” și „Rețele sociale” migrează în categoria de conținut pentru resurse Web „Medii comunicații Internet”.
- Regulile de acces la resurse Web bazate pe una sau mai multe categorii de conținut pentru resurse Web din listele „Magazine electronice” și „Sisteme de plată” migrează în categoria de conținut pentru resurse Web „Comerț electronic”.
- Regulile de acces la resurse Web bazate pe categoria de conținut pentru resurse Web „Jocuri de noroc” migrează în categoria de conținut „Jocuri de noroc, loterii, pronosport”.
- Regulile de acces la resurse Web bazate pe categoria de conținut pentru resurse Web „Jocuri în browser” migrează în categoria de conținut „Jocuri pe computer”.
- Regulile de acces la resurse Web bazate pe categorii de conținut pentru resurse Web care nu sunt cuprinse în lista de mai sus sunt migrate fără a se efectua modificări.

## Exportul și importul unei liste de adrese de resurse Web

Dacă ai creat o listă de adrese de resurse Web într-o regulă de acces la resurse Web, poți exporta această listă într-un fișier .txt. Ulterior, poți importa lista din acest fișier pentru a evita crearea manuală a unei liste noi de adrese de resurse Web la configurarea unei reguli de acces. Opțiunea de a exporta și, ulterior, de a importa lista de adrese de resurse Web poate fi utilă dacă, de exemplu, creezi reguli de acces cu parametri similari.

*Pentru a exporta o listă de adrese de resurse Web într-un fișier:*

1. Deschide [fereastra cu setările aplicației](#).



2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. Selectează regula a cărei listă de adrese de resurse Web dorești să o exporti într-un fișier.

4. Fă clic pe butonul **Editare**.

Se deschide fereastra **Regulă de acces la resurse Web**.

5. Dacă nu dorești să exporti întreaga listă de adrese de resurse Web, ci doar o parte a acesteia, selectează adresele de resurse Web necesare.

6. În partea dreaptă a câmpului cu lista de adrese de resurse Web, fă clic pe butonul .

Se deschide fereastra de confirmare a acțiunii.

7. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să exporti numai elementele selectate din lista de adrese de resurse Web, în fereastra de confirmare a acțiunii fă clic pe butonul **Da**.
- Dacă dorești să exporti numai elementele selectate din lista de adrese de resurse Web, în fereastra de confirmare a acțiunii fă clic pe butonul **Nu**.

Se deschide fereastra standard Microsoft Windows **Save as (Salvare ca)**.

8. În fereastra Microsoft Windows **Save as (Salvare ca)**, selectează fișierul în care dorești să exporti lista de adrese de resurse Web. Fă clic pe butonul **Salvare**.

*Pentru a importa lista de adrese de resurse Web dintr-un fișier într-o regulă:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.

În partea dreaptă a ferestrei se afișează setările componentei Control Web.

3. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să creezi o regulă de acces la resurse Web nouă, fă clic pe butonul **Adăugare**.
- Selectează regula de acces la resurse Web pe care dorești să o editezi. Apoi fă clic pe butonul **Editare**.

Se deschide fereastra **Regulă de acces la resurse Web**.

4. Efectuează una dintre următoarele acțiuni:

- Dacă creezi o regulă de acces la resurse Web nouă, selectează **Pentru adresele individuale** din lista verticală **Aplicare la adresele**.
- Dacă editezi o regulă de acces la resurse Web, mergi la pasul 5 al acestor instrucțiuni.

5. În partea dreaptă a câmpului cu lista de adrese de resurse Web, fă clic pe butonul .

Dacă creezi o regulă nouă, se deschide fereastra Microsoft Windows standard **Open file** (Deschidere fișier).

Dacă editezi o regulă, se deschide o fereastră în care ți se solicită confirmarea.

6. Efectuează una dintre următoarele acțiuni:

- Dacă editezi o regulă de acces la resurse Web nouă, mergi la pasul 7 al acestor instrucțiuni.
- Dacă editezi o regulă de acces la resurse Web, efectuează în fereastra de confirmare una dintre următoarele acțiuni:
  - Dacă dorești să adaugi elemente importate din lista de adrese de resurse Web la cele existente, fă clic pe butonul **Da**.
  - Dacă dorești să ștergi elementele existente din lista de adrese de resurse Web și să adaugi elementele importate, fă clic pe butonul **Nu**.

Se deschide fereastra Microsoft Windows standard **Open file** (Deschidere fișier).

7. În fereastra Microsoft Windows standard **Open file** (Deschidere fișier), selectează un fișier cu o listă de adrese de resurse Web de importat.

8. Fă clic pe butonul **Open** (Deschidere).

9. În fereastra **Regulă de acces la resurse Web**, fă clic pe **OK**.

## Editarea măștilor pentru adrese de resurse Web

Utilizarea unei *măști pentru adrese de resurse Web* (denumită și „mască de adresă”) poate fi utilă dacă ai nevoie să introduci multe adrese de resurse Web similare la crearea unei reguli de accesare a resurselor Web. Dacă este bine construită, o mască de adresă poate înlocui un număr mare de adrese de resurse Web.

Atunci când creezi o mască de adresă, respectă aceste reguli:

1. Caracterul \* înlocuiește orice secvență care conține zero sau mai multe caractere.

De exemplu, dacă introduceți masca de adrese \*abc\*, regula de acces este aplicată tuturor resurselor Web care conțin secvența abc. Exemplu: [http://www.exemplu.com/page\\_0-9abcdef.html](http://www.exemplu.com/page_0-9abcdef.html).

Pentru a include caracterul \* în masca de adresă, introdu caracterul \* de două ori.

2. Secvența de caractere `www.` de la începutul unei măști de adrese este interpretată ca o secvență `*.`

Exemplu: masca de adresă `www.exemplu.com` este tratată ca `*.exemplu.com`.

3. Dacă o mască de adrese nu are la început caracterul \*, conținutul măștii de adrese este echivalent cu același conținut cu prefixul `*`.

4. O secvență de caractere `*.` la începutul unei măști de adrese este interpretată ca `*.` sau ca un șir gol.

Exemplu: masca de adrese `http://www*.exemplu.com` acoperă adresa `http://www2.exemplu.com`.

5. Dacă o mască de adresă se termină cu alt caracter decât `/` sau `*`, conținutul măștii de adresă este echivalent cu același conținut cu postfixul `/*`.

Exemplu: masca de adrese `http://www.exemplu.com` acoperă adrese precum `http://www.exemplu.com/abc`, unde a, b și c sunt orice caractere.

6. Dacă o mască de adrese are la sfârșit caracterul `/`, conținutul măștii de adrese este echivalent cu același conținut cu postfixul `/*`.

7. Secvența de caractere `/*` la sfârșitul unei măști de adrese este interpretată ca `/*` sau ca un șir necompletat.

8. Adresele de resurse Web sunt comparate cu o mască de adrese, luându-se în considerare protocolul (`http` sau `https`):

- Dacă masca de adrese nu conține niciun protocol de rețea, această mască de adrese acoperă adresele fără niciun protocol de rețea.

Exemplu: masca de adrese `exemplu.com` acoperă adresele `http://exemplu.com` și `https://exemplu.com`.

- Dacă masca de adrese conține un protocol de rețea, această mască de adrese acoperă numai adresele cu același protocol de rețea ca și masca de adrese.

Exemplu: masca de adrese `http://*.exemplu.com` acoperă adresele `http://www.exemplu.com`, însă nu acoperă `https://www.exemplu.com`.

9. O mască de adresă încadrată între ghilimele este tratată fără a se lua în considerare alte înlocuiri suplimentare, cu excepția caracterului \* în cazul în care a fost inclus inițial în masca de adresă. Regulile 5 și 7 nu se aplică pentru măștile de adresă încadrate între ghilimele duble (vezi exemplele 14 – 18 din tabelul de mai jos).

10. Numele de utilizator și parola, portul de conectare și tipul majusculă/minusculă al caracterului nu sunt luate în considerare la compararea cu masca de adrese a unei resurse Web.

Exemple de moduri de utilizare a regulilor pentru crearea măștilor de adrese

Nr.	Mască de adrese	Adresă resursă Web de verificat	Este adresa acoperită de masca de adrese	Comentarii
1	*.exemplu.com	http://www.exemplu.com	Nu	Vezi 1.
2	*.exemplu.com	http://www.123.exemplu.com	Da	Vezi 1.
3	*exemplu.com	http://www.exemplu.com	Da	Vezi 1.
4	*exemplu.com	http://www.123.exemplu.com	Da	Vezi 1.
5	http://www.*.exemplu.com	http://www.exemplu.com	Nu	Vezi 1.
6	www.exemplu.com	http://www.exemplu.com	Da	Vezi 2, 1.
7	www.exemplu.com	https://www.exemplu.com	Da	Vezi 2, 1.
8	http://www.*.exemplu.com	http://123.exemplu.com	Da	Vezi 2, 4, 5.
9	www.exemplu.com	http://www.exemplu.com/abc	Da	Vezi 2, 5, 6.
10	exemplu.com	http://www.exemplu.com	Da	Vezi 3, 1.
11	http://exemplu.com/	http://exemplu.com/abc	Da	Vezi 6.
12	http://exemplu.com/*	http://exemplu.com	Da	Vezi 7.
13	http://exemplu.com	https://exemplu.com	Nu	Vezi 8.

14	"exemplu.com"	http://www.exemplu.com	Nu	Vezi 9.
15	"http://www.exemplu.com"	http://www.exemplu.com/abc	Nu	Vezi 9.
16	"*.exemplu.com"	http://www.exemplu.com	Da	Vezi 1, 9.
17	"http://www.exemplu.com/*"	http://www.exemplu.com/abc	Da	Vezi 1, 9.
18	"www.exemplu.com"	http://www.exemplu.com; https://www.exemplu.com	Da	Vezi 9, 8.
19	www.exemplu.com/abc/123	http://www.exemplu.com/abc	Nu	O m adre conț mult infor decă adre resu Web

## Editarea șabloanelor de mesaje ale componentei Control Web

În funcție de tipul de acțiune specificată în proprietățile regulilor pentru componenta Control Web, Kaspersky Endpoint Security afișează unul dintre următoarele tipuri de mesaje atunci când utilizatorii încearcă să acceseze resurse de pe Internet (aplicația înlocuiește o pagină HTML cu un mesaj pentru răspunsul din partea serverului HTTP):

- Mesaj de avertizare. Acest mesaj îl avertizează pe utilizator că vizitarea resursei Web nu se recomandă și/sau violează politica de securitate a companiei. Kaspersky Endpoint Security afișează un mesaj de avertizare dacă opțiunea **Avertizare** este selectată din lista verticală **Acțiune** din cadrul setărilor regulii care descrie resursa Web respectivă.

Dacă utilizatorul consideră că avertizarea este eronată, el poate face clic pe linkul din avertizare pentru a trimite un mesaj prestabilit către administratorul rețelei locale a companiei.

- Mesaj informativ cu privire la blocarea unei resurse Web. Kaspersky Endpoint Security afișează un mesaj informativ cu privire la blocarea unei resurse Web dacă opțiunea **Blocare** este selectată din lista verticală **Acțiune** din cadrul setărilor regulii care descrie resursa Web respectivă.

Dacă utilizatorul consideră că resursa Web este blocată în mod eronat, el poate face clic pe linkul din mesajul de notificare cu privire la blocarea resursei Web pentru a trimite un mesaj prestabilit către administratorul rețelei locale a companiei.

Pentru mesajul de avertizare, pentru mesajul informativ cu privire la blocarea unei resurse Web și pentru mesajul trimis către administratorul rețelei LAN sunt furnizate șabloane speciale. Poți modifica conținutul acestora.

*Pentru a modifica șablonul pentru mesajele componentei Control Web:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Control endpoint**, selectează subsecțiunea **Control Web**.  
În partea dreaptă a ferestrei se afișează setările componentei Control Web.
3. În partea dreaptă a ferestrei, fă clic pe butonul **Șabloane**.  
Se deschide fereastra **Șabloane de mesaje**.
4. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să editezi șablonul mesajului care îl avertizează pe utilizator împotriva vizitării unei resurse Web, selectează fila **Avertizare**.
  - Dacă dorești să editezi șablonul mesajului care informează utilizatorul asupra faptului că accesul la o resursă Web este blocat, selectează fila **Blocare**.
  - Pentru a edita șablonul mesajului trimis către administrator, selectează fila **Mesaj către administrator**.
5. Editează șablonul mesajului. De asemenea, poți folosi lista verticală **Variabilă**, precum și butoanele **Implicit** și **Link** (acest buton nu este disponibil în fila **Mesaj către administrator**).
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Senzor Kata Endpoint

Setările componentei Senzor KATA Endpoint sunt disponibile numai în Consola de administrare Kaspersky Security Center. Pentru a folosi această componentă, trebuie să instalezi plug-inul de administrare.

Această secțiune conține informații despre Senzorul KATA Endpoint și instrucțiuni despre cum se activează și dezactivează această componentă.

## Despre Senzorul Kata Endpoint

*Senzorul KATA Endpoint* este o componentă a Kaspersky Anti Targeted Attack Platform. Această soluție este destinată detectării rapide a amenințărilor de tipul atacurilor țintite.

Această componentă este instalată pe computere client. Pe aceste computere, componenta monitorizează continuu procese, conexiuni de rețea active și fișiere care sunt modificate și transmite aceste informații către Kaspersky Anti Targeted Attack Platform.

Funcționalitatea componentei este disponibilă pentru următoarele sisteme de operare:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Pentru informații suplimentare despre Kaspersky Anti Targeted Attack Platform care nu sunt furnizate în acest document, consultă secțiunea de ajutor de la Kaspersky Anti Targeted Attack Platform.

Conexiunile la intrare la computere pe care este instalată componenta Senzor KATA Endpoint trebuie să fie permise direct de la Serverul Kaspersky Anti Targeted Attack Platform indisponibil, fără un server proxy.

## Activarea sau dezactivarea componentei Senzor KATA Endpoint

*Pentru a activa sau a dezactiva componenta Senzor KATA Endpoint:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare relevant pentru care dorești să editezi setările politicii.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Setări avansate**, selectează subsecțiunea **Senzor KATA Endpoint**.
7. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi componenta Senzor KATA Endpoint, bifează caseta de selectare **Senzor KATA Endpoint**.
  - Dacă dorești să dezactivezi componenta Senzor KATA Endpoint, debifează caseta de selectare **Senzor KATA Endpoint**.
8. Dacă la pasul anterior ai bifat caseta de selectare **Senzor KATA Endpoint**, în câmpul **Adresă server**, specifică adresa serverului pentru Kaspersky Anti Targeted Attack Platform, formată din părțile următoare:
  - a. Nume protocol
  - b. Adresa IP a numelui de domeniu complet (FQDN) al serverului
  - c. Calea către Windows Event Collector pe server
9. Fă clic pe **OK**.
10. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

## Criptare date



În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută Microsoft Windows pentru stații de lucru, funcționalitatea de criptare a datelor este disponibilă complet. În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#), este disponibilă numai criptarea unităților de hard disk utilizându-se tehnologia Criptarea unitate BitLocker.

Această secțiune conține informații despre criptarea și decriptarea unităților de hard disk, a unităților amovibile și a fișierelor și directoarelor de pe unitățile locale ale computerului și furnizează instrucțiuni pentru configurarea și realizarea criptării și a decriptării datelor folosind Kaspersky Endpoint Security și plug-inul de administrare Kaspersky Endpoint Security.

Dacă nu există acces la date criptate, consultă instrucțiunile speciale pentru lucrul cu date criptate ([Lucrul cu fișiere criptate cu funcționalitate limitată de criptare a fișierelor](#), [Lucrul cu fișiere criptate dacă nu există acces la acestea](#)).

## Activarea afișării setărilor de criptare în politica aplicației Kaspersky Security Center

*Pentru a activa afișarea setărilor de criptare în politica aplicației Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În meniul contextual al nodului **Server de administrare – <Nume computer>** din arborele Consolei de administrare, selectează **Vizualizare** → **Setări interfață**.  
Se deschide fereastra **Setări interfață**.
3. În fereastra **Setări interfață**, bifează caseta de selectare **Afișare criptare și protecție date**.
4. Fă clic pe **OK**.

## Despre criptarea datelor

Kaspersky Endpoint Security îți permite să criptezi fișiere și directoare stocate pe unitățile locale și amovibile sau să criptezi întregi unități amovibile și unități de hard disk. Criptarea datelor reduce riscul pierderilor de informații atunci când un computer portabil, o unitate portabilă sau o unitate de hard disk este pierdută sau furată sau atunci când datele sunt accesate de către utilizatori sau aplicații neautorizate.

Dacă licența a expirat, aplicația nu criptează date noi, iar datele vechi criptate rămân criptate și sunt disponibile pentru utilizare. În acest caz, criptarea datelor noi necesită activarea programului cu o licență nouă care permite utilizarea criptării.

Dacă licența a expirat, Acordul de licență pentru utilizatorul final a fost încălcat sau s-a eliminat cheia, Kaspersky Endpoint Security sau componente de criptare, starea de criptare a fișierelor criptate anterior nu este garantată. Acest lucru se datorează faptului că unele aplicații, cum ar fi Microsoft Office Word, creează o copie temporară a fișierelor în cursul editării. Atunci când fișierul original este salvat, copia temporară înlocuiește fișierul original. Prin urmare, pe un computer care nu are funcționalitate de criptare sau aceasta este inaccesibilă, fișierul rămâne necriptat.

Kaspersky Endpoint Security oferă următoarele aspecte pentru protecția datelor:

- **Criptarea fișierelor de pe unitățile locale ale computerului.** Poți [compila liste de fișiere](#) după extensie sau după grupuri de extensii și liste de directoare stocate pe unitățile locale ale computerului și poți crea [reguli pentru criptarea fișierelor care sunt create de aplicații specifice](#). După aplicarea unei politici Kaspersky Security Center, Kaspersky Endpoint Security criptează și decriptează următoarele fișiere:

- Fișiere adăugate separat la liste pentru criptare și decriptare.
- Fișiere stocate în directoare adăugate la liste pentru criptare și decriptare.
- Fișiere create de aplicații separate.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

- **Criptarea unităților amovibile.** Poți specifica o regulă de criptare implicită, conform căreia aplicația execută aceeași acțiune asupra tuturor unităților amovibile sau poți specifica reguli de criptare pentru unități amovibile individuale.

Regula de criptare implicită are o prioritate mai mică decât regulile de criptare create pentru unități amovibile individuale. Regulile de criptare create pentru unități amovibile cu modelul de dispozitiv specificat au o prioritate mai mică decât regulile de criptare create pentru unități amovibile cu ID-ul de dispozitiv specificat.

Pentru a selecta o regulă de criptare pentru fișiere de pe o unitate amovibilă, Kaspersky Endpoint Security verifică dacă modelul și ID-ul dispozitivului sunt cunoscute sau nu. Aplicația efectuează apoi una dintre următoarele operațiuni:

- Dacă modelul de dispozitiv este cunoscut, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu modelul de dispozitiv specific.
- Dacă ID-ul de dispozitiv este cunoscut, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu ID-ul de dispozitiv specific.
- Dacă modelul și ID-ul de dispozitiv sunt cunoscute, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu ID-ul de dispozitiv specific. Dacă nu există o

astfel de regulă, dar există o regulă de criptare pentru unități amovibile cu modelul de dispozitiv specific, aplicația folosește această regulă. Dacă nu este specificată nicio regulă de criptare pentru ID-ul de dispozitiv specific și nici pentru modelul de dispozitiv specific, aplicația folosește recula de criptare implicită.

- Dacă nici modelul, nici ID-ul de dispozitiv nu sunt cunoscute, aplicația folosește regula de criptare implicită.

Aplicația îți permite să pregătești o unitate amovibilă pentru a folosi date criptate stocate pe ea în modul portabil. După activarea modului portabil, poți accesa fișiere criptate de pe unități amovibile conectate la un computer fără funcționalitate de criptare.

Aplicația efectuează acțiunea specificată în regula de criptare atunci când este aplicată politica aplicației Kaspersky Security Center.

- **Administrarea regulilor de acces al aplicațiilor la fișiere criptate.** Pentru orice aplicație poți crea o regulă de acces la fișiere criptate care blochează accesul la fișierele criptate sau care permite accesul la fișierele criptate doar ca text cifrat, o secvență de caractere obținute la aplicarea criptării.
- **Crearea arhivelor cifrate.** Poți crea arhive cifrate și poți proteja accesul la aceste arhive prin parolă. Conținutul arhivelor criptate poate fi accesat doar dacă sunt introduse parolele prin care protejezi accesul la arhivele respective. Aceste arhive pot fi transmise în mod sigur prin rețele sau pe unități amovibile.
- **Criptarea unităților de hard disk.** Poți selecta o tehnologie de criptare: Kaspersky Disk Encryption sau Criptare unitate BitLocker (denumită și „BitLocker”).

BitLocker este o tehnologie care face parte din sistemul de operare Windows. Dacă un computer este echipat cu un Trusted Platform Module (TPM), BitLocker îl folosește pentru a stoca cheile de recuperare care asigură accesul la o unitate de hard disk criptată. Atunci când computerul pornește, BitLocker solicită cheile de recuperare pentru unitatea de hard disk de la Trusted Platform Module și deblochează unitatea. Poți configura utilizarea unei parole și/sau a unui cod PIN pentru accesarea cheilor de recuperare.

Poți specifica regula de criptare implicită pentru unități de hard disk și poți crea o listă de unități de hard disk care să fie excluse de la criptare. Kaspersky Endpoint Security efectuează criptarea unităților de hard disk sector cu sector după ce este aplicată politica aplicației Kaspersky Security Center. Aplicația criptează toate partițiile logice ale unităților de hard disk simultan. Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

După ce unitățile de hard disk de sistem au fost criptate, la următoarea pornire a computerului utilizatorul trebuie să finalizeze autentificarea folosind [Agentul de Autentificare](#)  pentru ca unitățile de hard disk să poată fi accesate și sistemul de operare să fie încărcat. Acest lucru necesită introducerea parolei pentru simbolul sau cardul inteligent conectat la computer sau a numelui de utilizator și a parolei pentru contul de Agent de Autentificare creat de administratorul rețelei locale folosind activitățile de administrare pentru contul de Agent de Autentificare. Aceste conturi se bazează pe conturile Microsoft Windows sub care utilizatorii se conectează la sistemul de operare. Poți gestiona conturi de Agent de Autentificare și poți folosi tehnologia Single Sign-On (SSO), care îți permite să te conectezi automat la sistemul de operare folosind numele de utilizator și parola contului de Agent de Autentificare.

Dacă faci o copie de rezervă unui computer și apoi criptezi datele computerului, după care restaurezi copia de rezervă a computerului și criptezi datele computerului din nou, Kaspersky Endpoint Security creează dubluri ale conturilor Agent de Autentificare. Pentru a elimina conturile dublate, trebuie să folosești utilitarul `klmover` cu cheia `dupfix`. Utilitarul `klmover` este inclus în pachetul Kaspersky Security Center. Poți citi mai multe despre funcționarea sa în *Ghidul administratorului Kaspersky Security Center*.

Atunci când se efectuează upgrade la versiunea de aplicație la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, lista de conturi Agent de Autentificare nu este salvată.

Accesul la unități de hard disk criptate va fi posibil numai de pe computere pe care este instalat Kaspersky Endpoint Security cu [funcționalitate de criptare a unităților de hard disk](#). Această precauție reduce riscul pierderilor de date de pe o unitate de hard disk criptată atunci când se încearcă accesarea acesteia în afara rețelei locale a companiei.

Pentru a cripta unitățile de hard disk și unitățile amovibile, poți folosi funcția **Criptează doar spațiul de disc utilizat**. Se recomandă folosirea acestei funcții numai pentru dispozitive noi care nu au fost utilizate anterior. Dacă aplici criptarea unui dispozitiv aflat deja în uz, este recomandat să criptezi întregul dispozitiv. Astfel se asigură protecția tuturor datelor, chiar și a datelor șterse care pot conține informații ce pot fi recuperate.

Înainte de a începe criptarea, Kaspersky Endpoint Security obține o hartă cu sectoarele sistemului de fișiere. Primul val de criptare include sectoare care sunt ocupate de fișiere în momentul în care începe criptarea. Al doilea val de criptare include sectoare care au fost scrise după ce a început criptarea. După finalizarea criptării, toate sectoarele care conțin date sunt criptate.

După finalizarea criptării, dacă un utilizator șterge un fișier, sectoarele care au stocat fișierul devin disponibile pentru stocarea unor informații noi, la nivelul sistemului de fișiere, dar ele rămân în continuare criptate. Astfel, pe măsură ce noi fișiere sunt scrise pe un dispozitiv la lansarea criptării obișnuite cu funcția **Criptează doar spațiul de disc utilizat** activată pe computer, după un timp toate sectoarele vor fi criptate.

Datele necesare pentru decriptarea fișierelor The data sunt furnizate de serverul de administrare Kaspersky Security Center care controlează computerul la momentul criptării. În cazul în care computerul cu fișiere criptate se găsește sub controlul altui server de administrare din vreun motiv și fișierele criptate nu au fost accesate niciodată, accesul poate fi obținut în una din următoarele modalități:

- Solicită de la administratorul rețelei LAN acces la obiectele criptate.
- Restaurează date pe dispozitive criptate folosind Utilitarul de restaurare.
- Restaurează configurația serverului de administrare a Kaspersky Security Center care a controlat computerul la momentul criptării dintr-o copie de rezervă și utilizează această configurație pe serverul de administrare care controlează acum computerul cu obiectele criptate.

Aplicația creează fișiere de depanare în cursul criptării. Aproximativ 2-3% din spațiul liber nefragmentat de pe unitatea de hard disk este necesar pentru stocarea acestora. Dacă nu există suficient spațiu liber nefragmentat pe unitatea de hard disk, criptarea nu va începe până când nu eliberezi suficient spațiu.

Compatibilitatea dintre funcționalitatea de criptare a Kaspersky Endpoint Security și Kaspersky Anti-Virus for UEFI nu este asigurată. Criptarea unităților de hard disk pe computere pe care este instalat Kaspersky Anti-Virus for UEFI face această aplicație nefuncțională.

## Limitările funcționalității de criptare

Crearea partițiilor noi pe unități de hard disk criptate, precum și formatarea partițiilor existente de pe unități de hard disk criptate ar putea cauza pierderea datelor de pe aceste unități de hard disk.

Criptarea unităților de hard disk folosind tehnologia Kaspersky Disk Encryption nu este disponibilă pentru unitățile de hard disk care nu îndeplinesc cerințele hardware și software.

Kaspersky Endpoint Security nu acceptă următoarele configurații:

- Programul de încărcare pentru boot este amplasat pe o unitate, iar sistemul de operare pe o altă unitate.
- Sistemul conține software încorporat cu standardul UEFI 32.

- Intel Rapid Start Technology și unități care au o partiție dedicată pentru hibernare, chiar dacă tehnologia Intel Rapid Start Technology este dezactivată.
- Unități în format MBR cu mai mult de patru partiții extinse.
- Fișierul swap este amplasat pe o unitate non-sistem.
- Sistem multiboot cu mai multe sisteme de operare instalate simultan.
- Partiții dinamice (sunt acceptat doar partiții primare).
- Unități cu mai puțin de 2% spațiu-disk liber nefragmentat.
- Unități cu o dimensiune a sectorului alta decât 512 octeți sau 4096 de octeți care emulează 512 octeți.
- Unități hibride.

## Modificarea algoritmului de criptare

Algoritmul de criptare folosit de Kaspersky Endpoint Security pentru criptarea datelor depinde de bibliotecile de criptare incluse în kitul de distribuire.

*Pentru a schimba algoritmul de criptare:*

1. Decriptează obiectele pe care Kaspersky Endpoint Security le-a criptat înainte de a începe schimbarea algoritmului de criptare.

După schimbarea algoritmului de criptare, obiectele criptate anterior devine indisponibile.

2. [Elimină aplicația Kaspersky Endpoint Security.](#)
3. [Instalează Kaspersky Endpoint Security](#) din kitul de distribuire care conține bibliotecile de criptare pentru numere de biți diferite.

## Activarea tehnologiei Single Sign-On (SSO)

Tehnologia Single Sign-On (SSO) nu este compatibilă cu furnizori terți de acreditări de cont.

*Pentru a activa tehnologia Single Sign-On (SSO):*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să activezi tehnologia Single Sign-On (SSO).
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Setări de criptare comune**.
7. În subsecțiunea **Setări de criptare comune**, fă clic pe butonul **Configurare** în secțiunea **Setări parolă**.

Aceasta deschide fila **Agent de Autentificare** din fereastra **Setări parolă de criptare**.
8. Bifează caseta de selectare **Utilizare tehnologie Single Sign-On (SSO)**.
9. Fă clic pe **OK**.
10. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.
11. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

## Considerații speciale pentru criptarea fișierelor

Atunci când folosești funcționalitatea de criptare fișiere, reține următoarele aspecte:

- Politica aplicației Kaspersky Security Center cu setările implicite pentru criptarea unităților amovibile este formată pentru un grup specific de computere gestionate. Prin urmare, rezultatul aplicării politicii de criptare/decriptare fișiere pe unități amovibile depinde de computerul la care este conectată unitatea amovibilă.
- Kaspersky Endpoint Security nu criptează/decriptează fișiere care au starea Doar în citire și care sunt stocate pe unități amovibile.
- Kaspersky Endpoint Security criptează/decriptează fișiere din directoare predefinite numai pentru profiluri de utilizatori locali de pe sistemul de operare. Kaspersky Endpoint Security nu

criptează/decriptează fișiere din directoare predefinite pentru profiluri de utilizator în roaming, profiluri de utilizator obligatorii, profiluri de utilizator temporare și directoare redirecționate. Lista de directoare standard recomandate de Kaspersky pentru criptare include următoarele elemente:

- Documentele mele
  - Favorite
  - Cookie-uri
  - Desktop
  - Fișiere temporare de Internet Explorer
  - Fișiere temporare
  - Fișiere Outlook
- Kaspersky Endpoint Security nu efectuează criptarea fișierelor și a directoarelor atunci când această acțiune poate afecta sistemul de operare și aplicațiile instalate. De exemplu, următoarele fișiere și directoare și toate directoarele imbricate se regăsesc pe lista de excluderi de la criptare:
    - %WINDIR%.
    - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
    - Fișiere Windows registry.

Lista de excluderi de la criptare nu poate fi vizualizată sau editată. Chiar dacă se pot adăuga în lista de criptare fișiere și directoare aflate în lista de excluderi de la criptare, acestea nu vor fi criptate în cursul unei activități de criptare fișiere și directoare.

- Următoarele tipuri de dispozitive sunt acceptate ca unități amovibile:
  - Medii de date conectate prin magistrala USB
  - Unități de hard disk conectate prin magistralele USB și FireWire
  - Unități SSD conectate prin magistralele USB și FireWire

## Criptarea fișierelor de pe unitățile locale ale computerului



Criptarea fișierelor de pe unitățile locale ale computerului este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Criptarea fișierelor de pe unitățile locale ale computerului nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

Această secțiune se referă la criptarea fișierelor de pe unitățile locale ale computerului și conține instrucțiuni pentru configurarea și efectuarea criptării fișierelor pe unitățile locale ale computerului folosind Kaspersky Endpoint Security și plug-inul Consolă Kaspersky Endpoint Security.

## Criptarea fișierelor de pe unitățile locale ale computerului

*Pentru a cripta fișiere de pe unitățile locale:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi criptarea fișierelor de pe unități locale.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare fișiere și directoare**.
7. În partea dreaptă a ferestrei, selectează fila **Criptare**.
8. În lista verticală **Mod criptare**, selectează elementul **Reguli implicite**.
9. În fila **Criptare**, fă clic stânga pe butonul **Adăugare** și, în lista verticală, selectează unul dintre elementele următoare:
  - a. Selectați elementul **Directoare predefinite** pentru a adăuga la o regulă de criptare fișiere din directoare din profilurile utilizatorului local sugerate de experții Kaspersky.Se deschide fereastra **Selectare directoare predefinite**.

- b. Selectează elementul **Director particularizat** pentru a adăuga o cale de director introdusă manual la o regulă de criptare.

Apare fereastra **Adăugare director particularizat**.

- c. Selectează elementul **Fișiere după extensie** pentru a adăuga extensii de fișier la o regulă de criptare. Kaspersky Endpoint Security criptează fișierele cu extensiile specificate de pe toate unitățile locale ale computerului.

Apare fereastra **Adăugare/Editare listă de extensii de fișiere**.

- d. Selectează elementul **Fișiere după grupuri de extensii** pentru a adăuga grupuri de extensii de fișier la o regulă de criptare. Kaspersky Endpoint Security criptează fișierele care au extensiile listate în grupurile de extensii de pe toate unitățile locale ale computerului.

Apare fereastra **Selectare grupuri de extensii de fișiere**.

10. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.

11. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

Imediat după aplicarea politicii, Kaspersky Endpoint Security criptează fișierele care sunt incluse în regula de criptare și care nu sunt incluse în [regula de decriptare](#).

Dacă același fișier este adăugat a regula de criptare și al regula de decriptare, Kaspersky Endpoint Security nu criptează acest fișier dacă nu este criptat și îl decriptează dacă este criptat.

Kaspersky Endpoint Security criptează fișierele necriptate dacă proprietățile lor (cale fișier/nume fișier/extensie fișier) îndeplinesc după modificare criteriile regulii de criptare.

Kaspersky Endpoint Security amână criptarea fișierelor deschise până când acestea sunt închise.

Atunci când utilizatorul creează un fișier nou ale cărui proprietăți îndeplinesc criteriile regulii de criptare, Kaspersky Endpoint Security criptează fișierul imediat ce acesta este deschis.

Dacă muți un fișier criptat într-un alt director de pe unitatea locală, fișierul rămâne criptat indiferent dacă acest director este inclus sau nu în regula de criptare.

## Crearea regulilor de acces la fișiere criptate pentru aplicații

*Pentru a crea reguli de acces la fișiere criptate pentru aplicații:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare relevant pentru care dorești să configurezi reguli de acces la fișiere criptate pentru aplicații.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare fișiere și directoare**.
7. În lista verticală **Mod criptare**, selectează elementul **Reguli implicite**.

Regulile de acces sunt aplicate doar în modul **Reguli implicite**. După aplicarea regulilor de acces în modul **Reguli implicite**, dacă treci la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de acces. Toate aplicațiilor vor avea acces la toate fișierele criptate.

8. În partea dreaptă a ferestrei, selectează fila **Reguli pentru aplicații**.
9. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adăugare** și, în lista verticală, selectează elementul **Aplicații din lista Kaspersky Security Center**.

Se deschide fereastra **Adăugare aplicații din lista Kaspersky Security Center**.

Efectuează următoarele acțiuni:

- a. Specifică filtrele pentru a restrânge lista de aplicații din tabel. Pentru aceasta, specifică valorile pentru parametrii **Aplicație**, **Vânzător** și **Perioadă adăugată** și toate casetele de selectare din secțiunea **Grup**.
- b. Fă clic pe butonul **Reîmprospătare**.

Tabelul listează aplicații care corespund filtrelor aplicate.
- c. În coloana **Aplicații**, bifează casetele de selectare de lângă aplicațiile pentru care dorești să creezi reguli de acces la fișiere criptate.

d. În lista verticală **Regulă pentru aplicații**, selectează regula care va determina accesul aplicațiilor la fișiere criptate.

e. În lista verticală **Acțiuni pentru aplicații selectate anterior**, selectează acțiunea care trebuie efectuată de Kaspersky Endpoint Security pentru regulile de acces la fișiere criptate create anterior pentru aceste aplicații.

f. Fă clic pe **OK**.

Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

10. Dacă dorești să selectezi manual aplicații, fă clic pe butonul **Adăugare** și, în lista verticală, selectează elementul **Aplicații particularizate**.

Se deschide fereastra **Adăugare/editare nume de fișiere executabile ale aplicațiilor**.

Efectuează următoarele acțiuni:

a. În câmpul de introducere, tastează numele sau lista de nume de fișiere executabile ale aplicațiilor, inclusiv extensiile lor.

Mai poți adăuga numele fișierelor executabile ale aplicațiilor din lista Kaspersky Security Center făcând clic pe butonul **Adăugare din lista Kaspersky Security Center**.

b. Dacă este necesar, în câmpul **Descriere**, introdu o descriere a listei de aplicații.

c. În lista verticală **Regulă pentru aplicații**, selectează regula care va determina accesul aplicațiilor la fișiere criptate.

d. Fă clic pe **OK**.

Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

11. Fă clic pe **OK** pentru a salva modificările.

## Criptarea fișierelor create sau modificate de aplicații specifice

Poți crea o regulă prin care Kaspersky Endpoint Security va cripta toate fișierele create sau modificate de către aplicațiile specificate în regulă.

Fișierele care au fost create sau modificate de către aplicațiile specificate înainte de aplicarea regulii de criptare nu vor fi criptate.

*Pentru a configura criptarea fișierelor create sau modificate de aplicații specifice:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare relevant pentru care dorești să configurezi criptarea fișierelor create de aplicații specifice.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare fișiere și directoare**.
7. În lista verticală **Mod criptare**, selectează elementul **Reguli implicite**.

Regulile de criptare sunt aplicate doar în modul **Reguli implicite**. După aplicarea regulilor de criptare în modul **Reguli implicite**, dacă treci la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de criptare. Fișierele criptate anterior vor rămâne criptate.

8. În partea dreaptă a ferestrei, selectează fila **Reguli pentru aplicații**.
9. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adăugare** și, în lista verticală, selectează elementul **Aplicații din lista Kaspersky Security Center**.

Se deschide fereastra **Adăugare aplicații din lista Kaspersky Security Center**.

Efectuează următoarele acțiuni:

- a. Specifică filtrele pentru a restrânge lista de aplicații din tabel. Pentru aceasta, specifică valorile pentru parametrii **Aplicație**, **Vânzător** și **Perioadă adăugată** și toate casetele de selectare din secțiunea **Grup**.
- b. Fă clic pe butonul **Reîmprospătare**.

Tabelul listează aplicații care corespund filtrelor aplicate.
- c. În coloana **Aplicație**, bifează casetele de selectare de lângă aplicațiile ale căror fișiere create trebuie criptate.

d. În lista verticală **Regulă pentru aplicații**, selectează **Criptare globală fișiere create**.

e. În lista verticală **Acțiuni pentru aplicații selectate anterior**, selectează acțiunea care va fi efectuată de Kaspersky Endpoint Security pentru regulile de criptare fișiere care au fost formate anterior pentru aceste aplicații.

f. Fă clic pe **OK**.

Informațiile despre regulile de criptare pentru fișierele create sau modificate de către aplicațiile selectate apar în tabelul din fila **Reguli pentru aplicații**.

10. Dacă dorești să selectezi manual aplicații, fă clic pe butonul **Adăugare** și, în lista verticală, selectează elementul **Aplicații particularizate**.

Se deschide fereastra **Adăugare/editare nume de fișiere executabile ale aplicațiilor**.

Efectuează următoarele acțiuni:

a. În câmpul de introducere, tastează numele sau lista de nume de fișiere executabile ale aplicațiilor, inclusiv extensiile lor.

Mai poți adăuga numele fișierelor executabile ale aplicațiilor din lista Kaspersky Security Center făcând clic pe butonul **Adăugare din lista Kaspersky Security Center**.

b. Dacă este necesar, în câmpul **Descriere**, introdu o descriere a listei de aplicații.

c. În lista verticală **Regulă pentru aplicații**, selectează **Criptare globală fișiere create**.

d. Fă clic pe **OK**.

Informațiile despre regulile de criptare pentru fișierele create sau modificate de către aplicațiile selectate apar în tabelul din fila **Reguli pentru aplicații**.

11. Fă clic pe **OK** pentru a salva modificările.

## Generarea unei reguli de decriptare

*Pentru a genera o regulă de decriptare:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să generezi o listă de fișiere de decriptat.

3. În spațiul de lucru, selectează fila **Politici**.

4. Selectează politica necesară.

5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:

- În meniul contextual al politicii, selectează **Proprietăți**.
- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare fișiere și directoare**.

7. În partea dreaptă a ferestrei, selectează fila **Decriptare**.

8. În lista verticală **Mod criptare**, selectează elementul **Reguli implicite**.

9. În fila **Decriptare**, fă clic pe butonul **Adăugare** și, în lista verticală, selectează unul dintre elementele următoare:

- a. Selectați elementul **Directoare predefinite** pentru a adăuga la o regulă de decriptare fișiere din directoare din profilurile utilizatorului local sugerate de experții Kaspersky.

Se deschide fereastra **Selectare directoare predefinite**.

- b. Selectează elementul **Director particularizat** pentru a adăuga o cale de director introdusă manual la o regulă de decriptare.

Apare fereastra **Adăugare director particularizat**.

- c. Selectează elementul **Fișiere după extensie** pentru a adăuga extensii de fișier la o regulă de decriptare. Kaspersky Endpoint Security nu criptează fișierele cu extensiile specificate de pe toate unitățile locale ale computerului.

Apare fereastra **Adăugare/Editare listă de extensii de fișiere**.

- d. Selectează elementul **Fișiere după grupuri de extensii** pentru a adăuga grupuri de extensii de fișier la o regulă de decriptare. Kaspersky Endpoint Security nu criptează fișierele care au extensiile listate în grupurile de extensii de pe toate unitățile locale ale computerelor.

Apare fereastra **Selectare grupuri de extensii de fișiere**.

10. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.

11. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

Dacă același fișier este adăugat la regula de criptare și la regula de decriptare, Kaspersky Endpoint Security nu criptează acest fișier dacă nu este criptat și îl decriptează dacă este criptat.

# Decriptarea fișierelor de pe unitățile locale ale computerului

*Pentru a decrpta fișiere de pe unitățile locale:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi decriptarea fișierelor de pe unități locale.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare fișiere și directoare**.
7. În partea dreaptă a ferestrei, selectează fila **Criptare**.
8. Elimină fișierele și directoarele pe care dorești să le decriptezi din lista de criptare. Pentru aceasta, selectează fișierele și apoi selectează elementul **Ștergere regulă și decriptare fișiere** în meniul contextual al butonului **Eliminare**.

Poți șterge mai multe elemente simultan din lista de criptare. Pentru aceasta, în timp ce ții apăsată tasta **CTRL**, selectează fișierele de care ai nevoie făcând clic stânga pe ele și selectând elementul **Ștergere regulă și decriptare fișiere** în meniul contextual al butonului **Eliminare**.

Fișierele și directoarele eliminate din lista de criptare sunt adăugate în mod automat în lista de deciptare.
9. [Formează o listă de deciptare](#).
10. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.
11. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

Imediat ce politica este aplicată, Kaspersky Endpoint Security decriptează fișierele criptate care sunt adăugate la lista de deciptare.



Kaspersky Endpoint Security decriptează fișierele criptate dacă parametrii lor (cale fișier/nume fișier/extensie fișier) se modifică și corespund parametrilor obiectelor adăugate în lista de decriptare.

Kaspersky Endpoint Security amână decriptarea fișierelor deschise până când acestea sunt închise.

## Crearea pachetelor criptate

Kaspersky Endpoint Security nu efectuează nicio comprimare a fișierelor atunci când creează un pachet criptat.

*Pentru a crea un pachet criptat:*

1. Pe un computer pe care Kaspersky Endpoint Security este instalat, iar funcționalitatea de criptare este activată, folosește orice manager de fișiere pentru a selecta fișiere și/sau directoare pe care dorești să le adaugi la un pachet criptat. Fă clic dreapta pentru a deschide meniul contextual.
2. În meniul contextual, selectează **Adăugă la pachetul criptat**.  
Se deschide caseta de dialog standard Microsoft Windows **Alege o cale pentru salvarea pachetului criptat**.
3. În caseta de dialog standard Microsoft Windows **Alege o cale pentru salvarea pachetului criptat**, selectează o destinație pentru salvarea pachetului criptat pe unitatea amovibilă. Fă clic pe butonul **Salvare**.  
Se deschide fereastra **Adăugă la pachetul criptat**.
4. În fereastra **Adăugă la pachetul criptat**, tastează și confirmă o parolă.
5. Fă clic pe butonul **Creare**.  
Începe procesul de creare a pachetului criptat. Atunci când procesul se termină, este creat un pachet criptat, cu dezarhivare automată, protejat prin parolă, în directorul de destinație selectat pe unitatea amovibilă.

Dacă anulezi crearea unui pachet criptat, Kaspersky Endpoint Security execută următoarele operațiuni:

1. Termină procesul de copiere a fișierelor în pachet și termină toate operațiunile de criptare a pachetului în desfășurare, dacă există.
2. Elimină toate fișierele temporare care au fost create în cursul procesului de creare și criptare a pachetului și fișierul pachetului criptat în sine.
3. Îl notifică pe utilizator că procesul de creare a pachetului criptat a fost terminat forțat.

# Extragerea pachetelor criptate

*Pentru a extrage un pachet criptat:*

1. În orice manager de fișiere, selectează un pachet criptat. Fă clic pentru a lansa Expertul de dezarhivare.

Se deschide fereastra **Introducere parolă**.

2. Introdu parola care protejează pachetul criptat.

3. În fereastra **Introducere parolă**, fă clic pe **OK**.

Dacă parola este introdusă cu succes, se deschide caseta de dialog Microsoft Windows standard **Răsfoire**.

4. În caseta de dialog Microsoft Windows standard **Răsfoire**, selectează directorul de destinație în care va fi extras pachetul criptat și fă clic pe **OK**.

Începe procesul de extragere a pachetului criptat în directorul de destinație.

Dacă pachetul criptat a fost extras anterior în directorul de destinație specificat, fișierele existente în director vor fi suprascrise cu fișierele din pachetul criptat.

Dacă anulezi extragerea unui pachet criptat, Kaspersky Endpoint Security execută următoarele operațiuni:

1. Oprește procesul de decriptare a pachetului și termină toate operațiunile de copiere a fișierelor din pachetul criptat, dacă aceste operațiuni sunt în curs.
2. Șterge toate fișierele temporare create pe parcursul decriptării și extragerii pachetului criptat, precum și toate fișierele care au fost deja copiate din pachetul criptat în directorul de destinație.
3. Îl notifică pe utilizator că procesul de extragere a pachetului criptat a fost terminat forțat.

## Criptarea unităților amovibile

Criptarea unităților amovibile este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Criptarea unităților amovibile nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](https://support.kaspersky.com/KESWin/10SP2/ro-RO/all-in-one.htm).

Această secțiune conține informații despre criptarea unităților amovibile și instrucțiuni referitoare la configurarea și efectuarea criptării unităților amovibile cu Kaspersky Endpoint Security și plug-inul de administrare Kaspersky Endpoint Security.

## Lansarea criptării unităților amovibile

*Pentru a cripta unități amovibile:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi criptarea unităților amovibile.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități amovibile**.
7. În lista verticală **Mod criptare**, selectează acțiunea implicită care va fi executată de către Kaspersky Endpoint Security pentru toate unitățile amovibile care sunt conectate la computere din grupul de administrare selectat:
  - **Criptare unitate amovibilă în întregime**. Dacă este selectat acest element, atunci când se aplică politica aplicației Kaspersky Security Center cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security criptează conținutul unităților amovibile sector cu sector. Ca urmare, aplicația criptează nu doar fișierele stocate pe unități amovibile, dar și sistemele de fișiere de pe unitățile amovibile, inclusiv nume de fișiere și structura de directoare. Kaspersky Endpoint Security nu recriptează unități amovibile care au fost deja criptate.

Acest scenariu de criptare este permis de către funcționalitatea de criptare a unităților de hard disk a Kaspersky Endpoint Security.

- **Criptare toate fișierele**. Dacă este selectat acest element, atunci când se aplică politica aplicației Kaspersky Security Center cu setările de criptare specificate pentru unități

amovibile, Kaspersky Endpoint Security criptează toate fișierele care sunt stocate pe unitățile amovibile. Kaspersky Endpoint Security nu criptează din nou fișierele deja criptate. Aplicația nu criptează sistemele de fișiere ale unităților amovibile, inclusiv numele fișierelor structurilor de fișiere și de directoare criptate.

- **Criptare numai fișiere noi.** Dacă este selectat acest element, atunci când se aplică politica aplicației Kaspersky Security Center cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security criptează numai acele fișiere care au fost adăugate pe unitățile amovibile sau care au fost stocate pe unitățile amovibile și au fost modificate după ultima aplicare a politicii aplicației Kaspersky Security Center.
- **Decriptare unitate amovibilă în întregime.** Dacă este selectat acest element, atunci când se aplică politica aplicației Kaspersky Security Center cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security decriptează toate fișierele criptate care sunt stocate pe unitățile amovibile, precum și sistemele de fișiere ale unităților amovibile, dacă acestea au fost criptate anterior.

Acest scenariu de criptare este permis atât de către funcționalitatea de criptare a fișierelor, cât și de funcționalitatea de criptare a unităților de hard disk a Kaspersky Endpoint Security.

- **Lasă nemodificat.** Dacă este selectat acest element, atunci când se aplică politica aplicației Kaspersky Security Center cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security nu criptează și nu decriptează fișierele de pe unitățile amovibile.

8. [Creează](#) reguli de criptare pentru fișiere de pe unități amovibile al căror conținut dorești să-l criptezi.

9. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

Imediat ce politica este aplicată, atunci când utilizatorul conectează o unitate amovibilă sau dacă o unitate amovibilă este conectată deja, Kaspersky Endpoint Security notifică utilizatorul că unitatea amovibilă face obiectul unei reguli de criptare prin care datele stocate pe unitatea amovibilă și vor fi criptate.

Dacă este specificată regula *Lasă nemodificat* pentru criptarea datelor de pe o unitate amovibilă, aplicația nu afișează utilizatorului nicio notificare.

Aplicația îl avertizează pe utilizator că procesul de criptare poate dura ceva timp.

Aplicația îi solicită utilizatorului confirmarea operațiunii de criptare și efectuează următoarele acțiuni:

- Crijtează datele conform setărilor politicii, dacă utilizatorul este de acord cu criptarea.
- Lasă datele necrijtate, dacă utilizatorul respinge criptarea, și restricționează la numai în citire accesul la fișierele de pe unitatea amovibilă.
- Lasă datele necrijtate dacă utilizatorul ignoră solicitarea de criptare, restricționează accesul la fișierele de pe unitățile amovibile la numai în citire și solicită din nou utilizatorului să confirme criptarea datelor la următoarea aplicare a politicii Kaspersky Security Center sau conectare a unei unități amovibile.

Politica aplicației Kaspersky Security Center că setările implicite pentru criptarea datelor pe unități amovibile este formată pentru un grup specific de computere gestionate. Prin urmare, rezultatul criptării datelor de pe unități amovibile depinde de computerul la care este conectată unitatea amovibilă.

Dacă utilizatorul inițiază eliminarea în siguranță a unei unități amovibile în timpul criptării datelor, Kaspersky Endpoint Security întrerupe procesul de criptare a datelor și permite eliminarea unității amovibile înainte de finalizarea procesului de criptare.

În cazul în care criptarea unei unități amovibile a eșuat, vizualizați raportul **Crijtare date** în interfața Kaspersky Endpoint Security. Accesul la fișiere poate fi blocat de o altă aplicație. În acest caz, încercați să deconectați unitatea amovibilă de la computer și să o conectați din nou.

## Adăugarea unei reguli de criptare pentru unități amovibile

*Pentru a adăuga o regulă de criptare pentru unități amovibile:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să adaugi reguli de criptare unitate amovibilă.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.

- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități amovibile**.

7. Fă clic stânga pe butonul **Adăugare** în lista verticală și selectează unul dintre elementele următoare:

- Dacă dorești să adaugi reguli de criptare pentru unități amovibile care se găsesc în lista de dispozitive de încredere din componenta Control dispozitive, selectează **Din lista de dispozitive de încredere a acestei politici**.

Se deschide fereastra **Adăugare dispozitive din lista de dispozitive de încredere**.

- Dacă dorești să adaugi reguli de criptare pentru unități amovibile care sunt în lista Kaspersky Security Center, selectează **Din lista de dispozitive a Kaspersky Security Center**.

Se deschide fereastra **Toate dispozitivele din lista Kaspersky Security Center**.

8. Dacă ai selectat **Din lista de dispozitive a Kaspersky Security Center** la pasul anterior, specifică filtrele pentru afișarea dispozitivelor în tabel. Pentru aceasta:

- a. Specifică valorile pentru următorii parametri: **Afișare în tabel a dispozitivelor pentru care sunt definite următoarele, Tip dispozitiv, Nume, Computer și Kaspersky Disk Encryption**.

- b. Fă clic pe butonul **Reîmprospătare**.

9. În coloana **Tip dispozitiv**, bifează casetele de selectare de lângă numele unităților amovibile pentru care dorești să creezi reguli de criptare.

10. În lista verticală **Mod de criptare pentru dispozitivele selectate**, selectează acțiunea care va fi efectuată de către Kaspersky Endpoint Security asupra fișierelor stocate pe unitățile amovibile selectate.

11. Bifează caseta de selectare **Mod portabil** dacă dorești ca aplicația Kaspersky Endpoint Security să pregătească unitățile amovibile înainte de criptare, făcând posibilă utilizarea fișierelor criptate stocate pe ele în modul portabil.

Modul portabil îți permite să folosești fișiere criptate stocate pe unități amovibile care sunt conectate la computere [fără funcționalitatea de criptare](#).

12. Bifează caseta de selectare **Criptează doar spațiul de disc utilizat** dacă dorești ca aplicația Kaspersky Endpoint Security să creeze doar acele sectoare de disc care sunt ocupate de fișiere.

Dacă aplici criptarea unei unități aflate deja în uz, se recomandă să creezeți întreaga unitate. Astfel se asigură protecția tuturor datelor, chiar și a datelor șterse care pot conține informații ce pot fi recuperate. Funcția **Criptează doar spațiul de disc utilizat** este recomandată pentru unități noi care nu au fost folosite anterior.

Dacă un dispozitiv a fost criptat anterior folosind funcția **Criptează doar spațiul de disc utilizat**, după aplicarea unei politici în modul **Criptare unitate amovibilă în întregime**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

13. În lista verticală **Acțiuni pentru dispozitive selectate anterior**, selectează acțiunea care va fi efectuată de Kaspersky Endpoint Security în conformitate cu regulile de criptare care au fost definite anterior pentru unități amovibile:

- Dacă dorești ca regula de criptare creată anterior să rămână neschimbată, selectează **Omitere**.
- Dacă dorești ca o regulă de criptare creată anterior să fie înlocuită de noua regulă, selectează **Actualizare**.

14. Fă clic pe **OK**.

Liniile care conțin parametrii pentru regulile de criptare create apar în tabelul **Reguli particularizate**.

15. Fă clic pe **OK** pentru a salva modificările.

Regulile de criptare unitate amovibilă create sunt aplicate unităților amovibile conectate la orice computer controlat de politica modificată a Kaspersky Security Center.

## Editarea unei reguli de criptare pentru unități amovibile

*Pentru a edita o regulă de criptare pentru o unitate amovibilă:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să editezi o regulă de criptare pentru o unitate amovibilă.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități amovibile**.
7. În lista de unități amovibile pentru care au fost configurate reguli de criptare, selectează o înregistrare care corespunde unității amovibile de care ai nevoie.
8. Fă clic pe butonul **Setare regulă** pentru a edita regula de criptare pentru unitatea amovibilă selectată.  
  
Se deschide meniul contextual al butonului **Setare regulă**.
9. În meniul contextual al butonului **Setare regulă**, selectează acțiunea care va fi efectuată de către Kaspersky Endpoint Security asupra fișierelor stocate pe unitatea amovibilă selectată.
10. Fă clic pe **OK** pentru a salva modificările.

Regulile de criptare pentru unitate amovibilă adăugate sunt aplicate unităților amovibile conectate la orice computer controlat de politica modificată a Kaspersky Security Center.

## Activarea modului portabil pentru accesarea fișierelor criptate de pe unități amovibile

*Pentru a activa modul portabil pentru accesarea fișierelor criptate de pe unități amovibile:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să activezi modul portabil pentru accesare fișierelor criptate de pe unități amovibile.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități amovibile**.
7. Bifează caseta de selectare **Mod portabil**.

Modul portabil este disponibil pentru criptarea tuturor fișierelor sau doar a fișierelor noi.



8. Fă clic pe **OK**.

9. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

10. Conectează unitatea amovibilă la un dispozitiv pe care a fost aplicată politica Kaspersky Security Center.

11. Confirmă funcționarea criptării unității amovibile.

Se deschide o fereastră în care poți crea o parolă pentru [Manager de fișiere portabil ?](#)

12. Specifică o parolă care îndeplinește cerințele de complexitate și confirm-o.

13. Fă clic pe **OK**.

Kaspersky Endpoint Security criptează fișiere pe o unitate amovibilă în conformitate cu regulile de criptare definite în politica Kaspersky Security Center. Aplicația Manager de fișiere portabil utilizată pentru lucrul cu fișiere criptate va fi și ea scrisă pe unitatea amovibilă.

După activarea modului portabil, poți accesa fișiere criptate de pe unități amovibile conectate la un computer fără funcționalitate de criptare.

## Decriptarea unităților amovibile

*Pentru a decripta unități amovibile:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi decriptarea unităților amovibile.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități amovibile**.

7. Dacă dorești să decriptezi toate fișierele criptate stocate pe unități amovibile, în lista verticală **Mod criptare** selectează **Decriptare unitate amovibilă în întregime**.

8. Pentru a decripta datele stocate pe unități amovibile individuale, editează regulile de criptare pentru unitățile amovibile ale căror date dorești să le decriptezi. Pentru aceasta:

a. În lista de unități amovibile pentru care au fost configurate reguli de criptare, selectează o înregistrare care corespunde unității amovibile de care ai nevoie.

b. Fă clic pe butonul **Setare regulă** pentru a edita regula de criptare pentru unitatea amovibilă selectată.

Se deschide meniul contextual al butonului **Setare regulă**.

c. Selectează elementul **Decriptare toate fișierele** în meniul contextual al butonului **Setare regulă**.

9. Fă clic pe **OK** pentru a salva modificările.

10. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

După aplicarea politicii, atunci când utilizatorul conectează o unitate amovibilă sau dacă o unitate amovibilă este conectată deja, Kaspersky Endpoint Security notifică utilizatorul cu privire la faptul că unitatea amovibilă face obiectul regulii de criptare prin care fișierele stocate pe unitatea amovibilă și sistemul de fișiere al unității amovibile (dacă este criptat) vor fi decriptate. Aplicația îl avertizează pe utilizator că procesul de decriptare poate dura ceva timp.

Politica aplicației Kaspersky Security Center că setările implicite pentru criptarea datelor pe unități amovibile este formată pentru un grup specific de computere gestionate. Prin urmare, rezultatul decriptării datelor de pe unități amovibile depinde de computerul la care este conectată unitatea amovibilă.

Dacă utilizatorul inițiază eliminarea în siguranță a unei unități amovibile în timpul decriptării datelor, Kaspersky Endpoint Security întrerupe procesul de decriptare a datelor și permite eliminarea unității amovibile înainte de finalizarea operațiunii de decriptare.

În cazul în care decriptarea unei unități amovibile a eșuat, vizualizați raportul **Criptare date** în interfața Kaspersky Endpoint Security. Accesul la fișiere poate fi blocat de o altă aplicație. În acest caz, încercați să deconectați unitatea amovibilă de la computer și să o conectați din nou.

## Criptarea unităților de hard disk

În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută Microsoft Windows pentru stații de lucru, sunt disponibile Criptare unitate BitLocker și Kaspersky Disk Encryption pentru criptare. În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#), este disponibilă numai tehnologia Criptare unitate BitLocker.

Această secțiune conține informații despre criptarea unităților de hard disk și instrucțiuni referitoare la configurarea și efectuarea criptării unităților de hard disk cu Kaspersky Endpoint Security și plug-inul consolei Kaspersky Endpoint Security.

## Despre criptarea unităților de hard disk

Înainte de a începe criptarea unităților de hard disk, aplicația rulează o serie de verificări pentru a determina dacă dispozitivul poate fi criptat, ceea ce include verificarea unității de hard disk de sistem pentru a vedea dacă este compatibilă cu Agentul de Autentificare și cu componentele de criptare BitLocker. Pentru a verifica această compatibilitate, computerul trebuie repornit. După repornirea computerului, aplicația efectuează automat toate verificările necesare. Dacă verificarea compatibilității se încheie cu succes, activitatea de criptare a unităților de hard disk începe după încărcarea sistemului de operare și pornirea aplicației. Dacă se descoperă că unitatea de hard disk de sistem este incompatibilă cu Agentul de Autentificare sau componentele de criptare BitLocker, computerul trebuie pornit apăsând pe butonul hardware de resetare. Kaspersky Endpoint Security înregistrează în jurnal informațiile despre incompatibilitate. Pe baza acestor informații, aplicația nu începe criptarea unităților de hard disk la pornirea sistemului de operare. Informații despre acest eveniment sunt înregistrate în rapoartele Kaspersky Security Center.

Dacă s-a schimbat configurația hardware a computerului, informațiile despre incompatibilitate înregistrate în jurnal de către aplicație la precedenta verificare trebuie șterse pentru a verifica din nou compatibilitatea unității de hard disk de sistem cu Agentul de Autentificare și componentele de criptare BitLocker. Pentru aceasta, tastează înainte de criptarea unității de hard disk `avp pbatestreset` în linia de comandă. Dacă încărcarea sistemului de operare nu reușește după verificarea compatibilității unității de hard disk de sistem cu Agentul de Autentificare, [trebuie să ștergi obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare](#) folosind Utilitarul de restaurare și apoi trebuie să pornești Kaspersky Endpoint Security și să execuți din nou comanda `avp pbatestreset`.

După începerea criptării unității de hard disk, Kaspersky Endpoint Security criptează toate datele scrise pe unitățile de hard disk.

Dacă utilizatorul oprește sau repornește computerul în cursul decriptării unității de hard disk, Agentul de Autentificare se încarcă înainte de următoarea pornire a sistemului de operare. Kaspersky Endpoint Security reia criptarea unităților de hard disk după autentificarea cu succes în agentul de autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Hibernare în timpul criptării unităților de hard disk, Agentul de Autentificare se încarcă atunci când sistemul de operare revine din modul Hibernare. Kaspersky Endpoint Security reia criptarea unităților de hard disk după autentificarea cu succes în agentul de autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Repaus în timpul criptării unității de hard disk, Kaspersky Endpoint Security reia criptarea unităților de hard disk atunci când sistemul de operare revine din modul Hibernare, fără a încărca Agentul de Autentificare.

Autentificarea utilizatorului în Agentul de Autentificare poate fi efectuată în două moduri:

- Introdu numele de utilizator și parola pentru contul de Agent de Autentificare creat de administratorul rețelei LAN folosind instrumentele Kaspersky Security Center.
- Introdu parola pentru un simbol sau un simbol sau un card inteligent conectat la computer.

Agentul de Autentificare acceptă structuri de tastaturi pentru următoarele limbi:

- Engleză (Marea Britanie)
- Engleză (USA)
- Arabă (Algeria, Maroc, Tunisia; structură AZERTY)
- Spaniolă (America Latină)
- Italiană
- Germană (Germania și Austria)
- Germană (Elveția)
- Portugheză (Brazilia, structură ABNT2)
- Rusă (pentru tastaturi IBM/Windows cu 105 taste și structură QWERTY)
- Turcă (structură QWERTY)
- Franceză (Franța)
- Franceză (Elveția)
- Franceză (Belgia, structură AZERTY)
- Japoneză (pentru tastaturi cu 106 taste și structură QWERTY)

O structură de tastatură devine disponibilă în Agentul de Autentificare dacă acea structură a fost adăugată în setările de limbă și cele pentru standarde regionale din sistemul de operare și a devenit disponibilă în ecranul de bun venit din Microsoft Windows.

Dacă numele de cont din Agentul de Autentificare conține simboluri care nu pot fi introduse folosind structurile de tastatură disponibile în Agentul de Autentificare, unitățile de hard disk criptate pot fi accesate numai după ce sunt restaurate folosind [Unitarul de restaurare](#) sau după ce [numele de cont și parola pentru Agentul de Autentificare sunt restaurate](#).

Kaspersky Endpoint Security acceptă următoarele simboluri, cititoare de carduri inteligente și carduri inteligente:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (card inteligent)
- SafeNet eToken 4100 72K Java (card inteligent)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (card inteligent)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (cititor)
- Gemalto IDPrime .NET 511

# Criptarea unităților de hard disk folosind tehnologia Kaspersky Disk Encryption

Înainte de a cripta unitățile de hard disk pe un computer, îți recomandăm să te asiguri că respectivul computer nu este infectat. Pentru aceasta, începe o activitate [Scanare completă](#) sau [Scanare zone critice](#). Criptarea unității de hard disk a unui computer infectat de un rootkit poate duce la imposibilitatea funcționării acesteia.

*Pentru a cripta unitățile de hard disk folosind tehnologia Kaspersky Disk Encryption:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi criptarea unităților de hard disk.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități hard disk**.
7. În lista verticală **Tehnologie de criptare**, selectează opțiunea **Kaspersky Disk Encryption**.

Tehnologia Kaspersky Disk Encryption nu poate fi folosită dacă computerul are unități de hard disk criptate de BitLocker.

8. În lista verticală **Mod criptare**, selectează **Se criptează toate unitățile de hard disk**.

Dacă trebuie să excluzi unele unități de hard disk de la procesul de criptare, [creează o listă cu aceste unități de hard disk](#).

9. Selectează una dintre următoarele metode de criptare:

- Dacă dorești să aplici criptarea numai acelor sectoare de pe unitatea de hard disk care sunt ocupate de fișiere, bifează caseta de selectare **Criptează doar spațiul de disc utilizat**.

Dacă aplici criptarea unei unități aflate deja în uz, se recomandă să criptezi întreaga unitate. Astfel se asigură protecția tuturor datelor, chiar și a datelor șterse care pot conține informații ce pot fi recuperate. Funcția **Criptează doar spațiul de disc utilizat** este recomandată pentru unități noi care nu au fost folosite anterior.

- Dacă dorești să aplici criptarea întregii unități de hard disk, debifează caseta de selectare **Criptează doar spațiul de disc utilizat**.

Această funcție se aplică numai dispozitivelor necriptate. Dacă un dispozitiv a fost criptat anterior folosind funcția **Criptează doar spațiul de disc utilizat**, după aplicarea unei politici în modul **Se criptează toate unitățile de hard disk**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

10. Fă clic pe **OK** pentru a salva modificările.

11. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

## Criptarea unităților de hard disk folosind tehnologia Criptare unitate BitLocker

Înainte de a cripta unitățile de hard disk pe un computer, îți recomandăm să te asiguri că respectivul computer nu este infectat. Pentru aceasta, începe o activitate [Scanare completă](#) sau [Scanare zone critice](#). Criptarea unității de hard disk a unui computer infectat de un rootkit poate duce la imposibilitatea funcționării acesteia.

Este posibil ca utilizarea tehnologiei Criptare unitate BitLocker pe computere cu sistem de operare de server să necesite instalarea componentei **Criptare unitate BitLocker** utilizându-se expertul Adăugare roluri și componente.

*Pentru a cripta unitățile de hard disk folosind tehnologia Criptare unitate BitLocker:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi criptarea unităților de hard

disk.

3. În spațiul de lucru, selectează fila **Politici**.

4. Selectează politica necesară.

5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:

- În meniul contextual al politicii, selectează **Proprietăți**.
- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități hard disk**.

7. În lista verticală **Tehnologie de criptare**, selectează opțiunea **Criptare unitate BitLocker**.

8. În lista verticală **Mod criptare**, selectează opțiunea **Se criptează toate unitățile de hard disk**.

9. Dacă dorești să folosești pe un ecran tactil pentru a introduce informații într-un mediu preboot, bifează caseta de selectare **Permite utilizarea autentificării ce solicită intrarea de la tastatură înaintea încărcării sistemului pe tablete**.

Se recomandă să folosești această setare numai pentru dispozitivele care prezintă instrumente alternative pentru introducerea datelor, de exemplu o tastatură USB, într-un mediu preboot.

10. Selectează unul dintre următoarele tipuri de criptare:

- Dacă dorești să folosești criptarea hardware, bifează caseta de selectare **Utilizează criptare hardware**.
- Dacă dorești să folosești criptarea software, debifează caseta de selectare **Utilizează criptare hardware**.

11. Selectează una dintre următoarele metode de criptare:

- Dacă dorești să aplici criptarea numai acelor sectoare de pe unitatea de hard disk care sunt ocupate de fișiere, bifează caseta de selectare **Criptează doar spațiul de disc utilizat**.
- Dacă dorești să aplici criptarea întregii unități de hard disk, debifează caseta de selectare **Criptează doar spațiul de disc utilizat**.



Această funcție se aplică numai dispozitivelor necriptate. Dacă un dispozitiv a fost criptat anterior folosind funcția **Criptează doar spațiul de disc utilizat**, după aplicarea unei politici în modul **Se criptează toate unitățile de hard disk**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

12. Selectează o metodă pentru a accesa unitățile de hard disk care au fost criptate cu BitLocker.

- Dacă dorești să folosești un [Trusted Platform Module ?](#) (TPM) pentru a stoca cheile de criptare, selectează opțiunea **Utilizează Trusted Platform Module (TPM - Modul pentru platforme de încredere)**.
- Dacă nu folosești un Trusted Platform Module (TPM) pentru criptarea unităților de hard disk, selectează opțiunea **Utilizare parolă** și specifică numărul minim de caractere pe care trebuie să le conțină o parolă în câmpul **Lungime minimă parolă**.

Disponibilitatea unui modul TPM (Trusted Platform Module) este obligatorie pentru sistemele de operare Windows 7 și Windows 2008 R2, precum și pentru versiuni mai vechi.

13. Dacă ai selectat opțiunea **Utilizează Trusted Platform Module (TPM - Modul pentru platforme de încredere)** la pasul anterior:

- Dacă vrei să setezi un cod PIN care va fi solicitat atunci când utilizatorul încearcă să acceseze o cheie de criptare, bifează caseta de selectare **Utilizare cod PIN**, și, în câmpul **Lungime minimă a codului PIN**, specifică numărul minim de cifre pe care trebuie să le conțină un cod PIN.
- Dacă dorești acces la unități de hard disk criptate fără un modul Trusted Platform Module pe computer utilizând o parolă, bifează caseta de selectare **Utilizează parola dacă Trusted Platform Module (TPM) este indisponibil** și, în câmpul **Lungime minimă parolă**, indică numărul minim de caractere pe care trebuie să-l conțină parola.

În acest caz, accesul la chei de criptare va fi obținut utilizându-se parola respectivă la fel ca atunci când caseta de selectare **Utilizare parolă** ar fi bifată.

În cazul în care caseta de selectare **Utilizează parola dacă Trusted Platform Module (TPM) este indisponibil** nu este bifată și modulul Trusted Platform Module nu este disponibil, criptarea unității de hard disk nu va porni.

14. Fă clic pe **OK** pentru a salva modificările.

15. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

După aplicarea politicii pe computerul client cu aplicația Kaspersky Endpoint Security instalată, vor fi efectuate următoarele interogări:

- Dacă politica de criptare este aplicată unei unități de hard disk de sistem, va apărea fereastra pentru codul PIN dacă este utilizat modulul Trusted Platform Module, iar, în caz contrar, va apărea fereastra de solicitare a parolei pentru autorizarea preîncărcării.
- Dacă sistemul de operare al computerului are activat modul de compatibilitate standard Federal Information Processing, atunci, în Windows 8 și versiuni ulterioare, sistemul de operare va afișa o fereastră de solicitare de conectare la un dispozitiv USB pentru salvarea fișierului cheie de recuperare.

Dacă nu există acces la chei de criptare, utilizatorul îi poate solicita administratorului rețelei locale să-i furnizeze o [cheie de recuperare](#) (în cazul în care cheia de recuperare nu a fost salvată anterior pe dispozitivul USB sau a fost pierdută).

## Crearea unei liste de unități de hard disk excluse de la criptare

Poți crea o listă de excluderi de la criptare numai pentru tehnologia Kaspersky Disk Encryption.

*Pentru a crea o listă de unități de hard disk excluse de la criptare:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să creezi o listă de unități de hard disk de exclus de la criptare.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități hard disk**.

7. În lista verticală **Tehnologie de criptare**, selectează opțiunea **Kaspersky Disk Encryption**.

Înregistrările care corespund unităților de hard disk excluse de la criptare apar în tabelul **Nu se criptează următoarele unități hard disk**. Acest tabel este gol dacă nu ai format anterior o listă de unități de hard disk care să fie excluse de la criptare.

8. Pentru a adăuga unități de hard disk noi la lista de unități de hard disk excluse de la scanare:

a. Fă clic pe butonul **Adăugare**.

Se deschide fereastra **Toate dispozitivele din lista Kaspersky Security Center**.

b. În fereastra **Toate dispozitivele din lista Kaspersky Security Center**, specifică valorile pentru următorii parametri: **Nume**, **Computer**, **Tip de disc** și **Kaspersky Disk Encryption**.

c. Fă clic pe butonul **Reîmprospătare**.

d. În coloana **Nume**, bifează casetele de selectare din rândurile tabelului care corespund unităților de hard disk pe care dorești să le adaugi la lista de unități de hard disk excluse de la criptare.

e. Fă clic pe **OK**.

Unitățile de hard disk selectate apar în tabelul **Nu se criptează următoarele unități hard disk**.

9. Dacă dorești să elimini unități de hard disk din tabelul de excluderi, selectează una sau mai multe linii în tabelul **Nu se criptează următoarele unități hard disk** și fă clic pe butonul **Ștergere**.

Pentru a selecta linii multiple în tabel, selectează-le în timp ce ții apăsată tasta **CTRL**.

10. Fă clic pe **OK** pentru a salva modificările.

## Decriptarea unităților de hard disk

Poți decrpta unități d hard disk chiar dacă nu există nicio licență activă care permite criptarea datelor.

*Pentru a decrpta unități de hard disk:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi decriptarea unităților de hard disk.

3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Criptare unități hard disk**.
7. În lista verticală **Tehnologie de criptare**, selectează tehnologia cu care vor fi criptate unitățile de hard disk.
8. Efectuează una dintre următoarele acțiuni:
  - În lista verticală **Mod criptare**, selectează opțiunea **Se decriptează toate unitățile hard disk** dacă dorești să decriptezi toate unitățile de hard disk criptate.
  - [Adaugă](#) unitățile de hard disk criptate pe care dorești să le decriptezi în tabelul **Nu se criptează următoarele unități hard disk**.

Această opțiune este disponibilă numai pentru tehnologia Kaspersky Disk Encryption.

9. Fă clic pe **OK** pentru a salva modificările.

10. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

Dacă utilizatorul închide sau repornește computerul în timpul decriptării unităților de hard disk care au fost criptate utilizându-se tehnologia Kaspersky Disk Encryption, Agentul de Autentificare se încarcă înainte de următoarea pornire a sistemului de operare. Kaspersky Endpoint Security reia criptarea unității de hard disk după autentificarea cu succes în agentul de autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Hibernare în timpul decriptării unităților de hard disk care au fost criptate utilizându-se tehnologia Kaspersky Disk Encryption, Agentul de Autentificare se încarcă atunci când sistemul de operare revine din modul Hibernare. Kaspersky Endpoint Security reia criptarea unității de hard disk după autentificarea cu succes în agentul de autentificare și pornirea cu succes a sistemului de operare. După decriptarea unității de hard disk, modul Hibernare nu mai este disponibil până la următoarea rebootare a sistemului de operare.

Dacă sistemul de operare trece în modul Repaus în timpul decriptării unității de hard disk, Kaspersky Endpoint Security reia decriptarea unităților de hard disk atunci când sistemul de operare revine din modul Hibernare, fără a încărca Agentul de Autentificare.

## Gestionarea Agentului de Autentificare

Dacă unitățile de hard disk de sistem sunt criptate, Agentul de autentificare se încarcă înainte de pornirea sistemului de operare. Utilizează Agentul de autentificare pentru a finaliza autentificarea și a obține accesul la unități de hard disk de sistem criptate și a încărca sistemul de operare.

După finalizarea cu succes a procedurii de autentificare, se încarcă sistemul de operare. Procesul de autentificare se repetă de fiecare dată când sistemul de operare repornește.

În unele cazuri este posibil ca utilizatorul să nu poată transmite autentificarea. De exemplu, autentificarea este imposibilă dacă utilizatorul a uitat acreditările pentru contul de Agent de Autentificare sau parola pentru simbol sau cardul inteligent ori dacă a pierdut simbolul sau cardul inteligent.

Dacă utilizatorul uitat acreditările pentru contul de Agent de Autentificare sau parola pentru simbol sau cardul inteligent, trebuie să contacteze administratorul rețelei LAN a companiei [pentru a le recupera](#).

Dacă un utilizator a pierdut un simbol sau un card inteligent, administratorul trebuie [să adauge fișierul unui certificat electronic pentru simbol sau card inteligent](#) la comanda pentru crearea unui cont de Agent de Autentificare. Apoi utilizatorul trebuie să finalizeze procedura pentru [restaurarea datelor pe dispozitive criptate](#).

## Folosirea unui simbol/card inteligent cu Agentul de Autentificare

Un simbol sau un card inteligent poate fi folosit pentru autentificare atunci când se accesează unități de hard disk criptate. Pentru aceasta, trebuie să adaugi fișierul certificatului electronic al unui simbol sau card inteligent la comanda pentru crearea unui cont de Agent de Autentificare.

Folosirea unui simbol sau card inteligent este disponibilă dacă unitățile de hard disk ale computerului au fost criptate utilizându-se algoritmul de criptare AES256. În cazul în care unitățile de hard disk ale computerului a fost criptate utilizându-se algoritmul de criptare AES56, adăugarea fișierului de certificat electronic la comandă va fi refuzată.

Pentru a adăuga fișierul certificatului electronic al unui simbol sau card inteligent la comanda de creare a unui cont de Agent de Autentificare, mai întâi trebuie să salvezi fișierul folosind software terț pentru administrarea certificatelor.

Certificatul simbolului sau al cardului inteligent trebuie să aibă următoarele proprietăți:

- Certificatul trebuie să fie conform cu standardul X.509 și fișierul certificatului trebuie să aibă codificarea DER.

Dacă certificatul electronic al simbolului sau al cardului inteligent nu îndeplinește această cerință, plug-inul de administrare nu va încărca acest certificat în comanda pentru crearea unui cont de Agent de Autentificare și va afișa un mesaj de eroare.

- Parametrul KeyUsage care definește scopul certificatului trebuie să aibă valoarea keyEncipherment sau dataEncipherment.

Dacă certificatul electronic al simbolului sau al cardului inteligent nu îndeplinește această cerință, plug-inul de administrare va încărca acest certificat în comanda pentru crearea unui cont de Agent de Autentificare și va afișa un mesaj de avertizare.

- Certificatul conține o cheie RSA cu o lungime de cel puțin 1024 de biți.

Dacă certificatul electronic al simbolului sau al cardului inteligent nu îndeplinește această cerință, plug-inul de administrare nu va încărca acest certificat în comanda pentru crearea unui cont de Agent de Autentificare și va afișa un mesaj de eroare.

## Editarea mesajelor de ajutor ale Agentului de Autentificare

Înainte de a edita mesajele de ajutor ale Agentului de Autentificare, recitește [lista caracterelor acceptate într-un mediu preboot](#).

*Pentru a edita mesajele de ajutor ale Agentului de Autentificare:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să editezi mesajele de ajutor ale Agentului de Autentificare.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Criptare date**, selectează subsecțiunea **Setări de criptare comune**.

7. În secțiunea **Șabloane**, fă clic pe butonul **Ajutor**.

Această acțiune deschide fereastra **Mesaje de ajutor pentru Agentul de Autentificare**.

8. Efectuează următoarele acțiuni:

- Selectează fila **Autentificare** pentru a edita textul de ajutor afișat în fereastra Agentului de Autentificare atunci când sunt introduse acreditările contului.
- Selectează fila **Modificare parolă** pentru a edita textul de ajutor afișat în fereastra Agentului de autentificare atunci când parola pentru contul de Agent de Autentificare este modificată.
- Selectează fila **Recuperare parolă** pentru a edita textul de ajutor afișat în fereastra Agentului de autentificare atunci când parola pentru contul de Agent de Autentificare este recuperată.

9. Editează mesajele de ajutor.

Dacă dorești să restaurezi textul original, fă clic pe butonul **Implicit**.

10. Fă clic pe **OK**.

11. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.

## Suport limitat pentru caractere în mesajele de ajutor pentru Agentul de Autentificare

Într-un mediu preboot, sunt acceptate următoarele caractere Unicode:

- Alfabetul latin de bază (0000 - 007F)
- Caractere suplimentare Latin-1 (0080 - 00FF)
- Caractere extinse Latin-A (0100 - 017F)
- Caractere extinse Latin-B (0180 - 024F)
- Caractere ID extinse necombinate (02B0 - 02FF)
- Semne diacritice combinate (0300 - 036F)
- Alfabetele grecesc și cel copt (0370 - 03FF)
- Chirilic (0400 - 04FF)
- Ebraic (0590 - 05FF)

- Script arabic (0600 - 06FF)
- Caractere latine suplimentare extinse (1E00 - 1EFF)
- Semne de punctuație (2000 - 206F)
- Simboluri de monede (20A0 - 20CF)
- Simboluri de tip literă (2100 - 214F)
- Figuri geometrice (25A0 - 25FF)
- Forme de prezentare din setul arab script-B (FE70 - FEFF)

Caracterele care nu sunt specificate în această listă nu sunt acceptate într-un mediu preboot. Nu se recomandă utilizarea acestor caractere în mesajele de ajutor pentru Agentul de Autentificare.

## Selectarea nivelului de urmărire pentru Agentul de Autentificare

Aplicația înregistrează în jurnal informațiile de serviciu despre funcționarea Agentului de Autentificare și informații despre operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire. Fișierul de urmărire al Agentului de Autentificare poate fi foarte de util atunci când trebuie să [restaurezi date pe unități de hard disk criptate](#).

*Pentru a selecta un nivel de urmărire pentru Agentul de Autentificare:*

1. Imediat ce computerul cu unitățile de hard disk criptate este pornit, apasă pe butonul **F3** pentru a apela o fereastră pentru configurarea setărilor Agentului de Autentificare.
2. Selectează nivelul de urmărire în fereastra de setări a Agentului de Autentificare:
  - **Dezactivare înregistrare în jurnal depanare (implicit).** Dacă este selectată această opțiune, aplicația nu înregistrează în jurnal informațiile despre evenimentele Agentului de Autentificare în fișierul de urmărire.
  - **Activare înregistrare în jurnal depanare.** Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire.
  - **Activare înregistrare detaliată în jurnal.** Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile detaliate despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire.



Nivelul de detalii pentru înregistrările efectuate cu această opțiune este mai mare în comparație cu nivelul pentru opțiunea **Activare înregistrare în jurnal depanare**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

- **Activare înregistrare în jurnal depanare și selectare port serial.** Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire și transmite aceste informații prin portul COM.

Dacă un computer cu unități de hard disk criptate este conectat la un alt computer prin portul COM, evenimentele Agentului de Autentificare pot fi examinate de pe celălalt computer.

- **Activare înregistrare detaliată în jurnal depanare și selectare port serial.** Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile detaliate despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire și transmite aceste informații prin portul COM.

Nivelul de detalii pentru înregistrările efectuate cu această opțiune este mai mare în comparație cu nivelul pentru opțiunea **Activare înregistrare în jurnal depanare și selectare port serial**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

Datele sunt înregistrate în fișierul de urmărire al Agentului de Autentificare dacă există unități de hard disk criptate pe computer sau în cursul criptării unităților de hard disk.

Fișierul de urmărire al Agentului de Autentificare nu este trimis către Kaspersky, spre deosebire de alte fișiere de urmărire ale aplicației. Dacă este necesar, administratorul de sistem poate trimite manual fișierul de urmărire al Agentului de Autentificare către Kaspersky pentru analiză.

## Gestionarea conturilor Agentului de Autentificare

Următoarele instrumente Kaspersky Security Center sunt disponibile pentru gestionarea conturilor de Agent de Autentificare:

- Activitate de grup pentru gestionarea conturilor de Agent de Autentificare. Această activitate îți permite să gestionezi conturile de Agent de Autentificare pentru un grup de computere client.
- Activitatea locală **Criptare (gestionare cont)**. Această activitate îți permite să gestionezi conturile de Agent de Autentificare pentru computere client individuale.

*Pentru a configura setările pentru activitatea de gestionare conturi de Agent de Autentificare:*

1. Creează ([Crearea unei activități locale](#), [Crearea unei activități de grup](#)) o activitate de gestionare a contului de Agent de Autentificare.
2. [Deschide](#) secțiunea **Setări** în fereastra **Proprietăți: <numele activității de gestionare pentru contul de Agent de Autentificare>**.
3. [Adaugă comenzi pentru crearea unui cont de Agent de Autentificare](#).
4. [Adaugă comenzi pentru editarea unui cont de Agent de Autentificare](#).
5. [Adaugă comenzi pentru ștergerea conturilor de Agent de Autentificare](#).
6. Dacă este nevoie, editează comenzile adăugate pentru gestionarea conturilor de Agent de Autentificare. Pentru aceasta, selectează o comandă în tabelul **Comenzi pentru administrarea conturilor de Agent de Autentificare** și fă clic pe butonul **Editare**.
7. Dacă este nevoie, șterge comenzile adăugate pentru gestionarea conturilor de Agent de Autentificare. Pentru aceasta, selectează una sau mai multe comenzi în tabelul **Comenzi pentru administrarea conturilor de Agent de Autentificare** și fă clic pe butonul **Eliminare**.

Pentru a selecta linii multiple în tabel, selectează-le în timp ce ții apăsată tasta **CTRL**.

8. Pentru a salva modificările, fă clic pe **OK** în fereastra de proprietăți a activității.
9. [Execută activitatea](#).

Comenzile de gestionare a conturilor de Agent de Autentificare adăugate la activitate vor fi executate.

## Adăugarea unei comenzi pentru crearea unui cont de Agent de Autentificare

*Pentru a adăuga o comandă pentru crearea unui cont de Agent de Autentificare:*

1. [Deschide](#) secțiunea **Setări** în fereastra **Proprietăți: <numele activității de gestionare pentru contul de Agent de Autentificare>**.
2. Fă clic pe butonul **Adăugare** și, în lista verticală, selectează **Comandă de adăugare cont**.  
Apare fereastra **Adăugare cont de utilizator**.

3. În câmpul **Adăugare cont de utilizator** din fereastra **Cont Windows**, specifică numele contului Microsoft Windows pe baza căruia va fi creat un cont de Agent de Autentificare.

Pentru aceasta, tastează manual numele contului sau fă clic pe butonul **Selectare**.

4. Dacă ai introdus manual numele unui cont Microsoft Windows, fă clic pe butonul **Permitere** pentru a determina identificatorul de securitate (SID) al contului.

Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

Determinarea SID-ului contului Microsoft Windows atunci când se adaugă comanda de creare a unui cont de Agent de Autentificare reprezintă un mod convenabil să te asiguri că numele contului Microsoft Windows introdus manual este corect. În cazul în care contul Microsoft Windows introdus nu există sau aparține unui domeniu care nu este de încredere sau nu se află pe computerul pentru care este modificată activitatea locală **Criptare (administrare cont)**, activitatea pentru administrarea contului de Agent de autentificare se termină cu o eroare.

5. Bifează caseta de selectare **Schimbați contul de utilizator curent** pentru a înlocui un cont denumit identic creat anterior pentru Agentul de Autentificare cu contul creat acum.

Acest pas este disponibil atunci când adaugi o comandă de creare pentru contul de Agent de Autentificare în proprietățile unei activități de grup pentru administrarea conturilor de Agent de Autentificare. Acest pas nu este disponibil dacă adaugi o comandă de creare pentru contul de Agent de Autentificare în proprietățile unei activități locale **Criptare (administrare cont)**.

6. În câmpul **Nume utilizator**, tastează numele contului de Agent de Autentificare care trebuie introdus în cursul autentificării pentru a accesa unitățile de hard disk criptate.
7. Bifează caseta de selectare **Permitere autentificare pe bază de parolă** dacă dorești ca aplicația să solicite utilizatorului introducerea parolei de cont de Agent de Autentificare în cursul autentificării pentru a accesa unitățile de hard disk criptate.
8. Dacă ai bifat caseta de selectare **Permitere autentificare pe bază de parolă** la pasul anterior:
- În câmpul **Parolă**, tastează parola pentru contul de Agent de Autentificare care trebuie introdusă în cursul autentificării pentru a accesa unitățile de hard disk criptate.
  - În câmpul **Confirmare parolă**, confirmă parola pentru contul de Agent de Autentificare introdusă în pasul anterior.
  - Efectuează una dintre următoarele acțiuni:

- Selectează opțiunea **Modificare parolă la prima autentificare** dacă dorești ca aplicația să afișeze o solicitare de modificare a parolei utilizatorului care se autentifică pentru prima dată cu contul specificat în comandă.
  - În caz contrar, selectează opțiunea **Nu necesită modificarea parolei**.
9. Bifează caseta de selectare **Permitere autentificare pe bază de certificat** dacă dorești ca aplicația să solicite utilizatorului să conecteze un simbol sau un card inteligent la computer în cursul procesului de autentificare, pentru a accesa unitățile de hard disk criptate.
10. Dacă ai bifat caseta de selectare **Permitere autentificare pe bază de certificat** în pasul anterior, fă clic pe butonul **Răsfoire** și selectează fișierul certificatului electronic al simbolului sau cardului inteligent în fereastra **Selectare fișier de certificat**.
11. Dacă este nevoie, în câmpul **Descriere comandă**, introdu detaliile pentru contul de Agent de Autentificare de care ai nevoie pentru administrarea comenzii.
12. Efectuează una dintre următoarele acțiuni:
- Bifează caseta de selectare **Permitere autentificare** dacă dorești ca aplicația să permită utilizatorului care lucrează sub contul specificat în comandă accesul la dialogul de autentificare în Agentul de Autentificare.
  - Bifează caseta de selectare **Blocare autentificare** dacă dorești ca aplicația să blocheze utilizatorului care lucrează sub contul specificat în comandă accesul la dialogul de autentificare în Agentul de Autentificare.

13. În fereastra **Adăugare cont de utilizator**, fă clic pe **OK**.

## Adăugarea comenzii de editare pentru un cont de Agent de Autentificare

*Pentru a adăuga o comandă pentru editarea unui cont de Agent de Autentificare:*

1. În secțiunea **Setări** din fereastra **Proprietăți: <numele activității de administrare pentru contul de Agent de Autentificare>**, deschide meniul contextual al butonului **Adăugare** și selectează elementul **Comandă de editare cont**.  
Apare fereastra **Editare cont utilizator**.
2. În câmpul **Cont Windows** din fereastra **Editare cont utilizator**, specifică numele contului de utilizator Microsoft Windows care a fost folosit pentru a crea contul de Agent de Autentificare pe care dorești să-l editezi. Pentru aceasta, tastează manual numele contului sau fă clic pe butonul **Selectare**.

3. Dacă ai introdus manual numele unui cont de utilizator Microsoft Windows, fă clic pe butonul **Permitere** pentru a determina identificatorul de securitate (SID) contului de utilizator.

Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

Determinarea SID-ului contului de utilizator Microsoft Windows atunci când se adaugă comanda de editare pentru un cont de Agent de Autentificare reprezintă un mod convenabil să te asiguri că numele contului de utilizator Microsoft Windows introdus manual este corect. În cazul în care contul de utilizator Microsoft Windows nu există sau aparține unui domeniu care nu este de încredere, activitatea de grup pentru administrarea conturilor de Agent de autentificare se termină cu o eroare.

4. Bifează caseta de selectare **Modificare nume utilizator** și introdu un nume nou pentru contul de Agent de autentificare dacă dorești ca aplicația Kaspersky Endpoint Security să modifice numele de utilizator pentru toate conturile de Agent de autentificare create folosind contul Microsoft Windows cu numele indicat în câmpul **Cont Windows** cu numele introdus în câmpul de mai jos.
5. Bifează caseta de selectare **Modificare setări de autentificare bazată pe parolă** pentru ca setările de autentificare bazate pe parolă să poată fi editate.
6. Bifează caseta de selectare **Permitere autentificare pe bază de parolă** dacă dorești ca aplicația să solicite utilizatorului introducerea parolei de cont de Agent de Autentificare în cursul autentificării pentru a accesa unitățile de hard disk criptate.
7. Dacă ai bifat caseta de selectare **Permitere autentificare pe bază de parolă** la pasul anterior:
  - a. În câmpul **Parolă**, introdu noua parolă pentru contul de Agent de Autentificare.
  - b. În câmpul **Confirmare parolă**, confirmă parola introdusă în pasul anterior.
8. Bifează caseta de selectare **Editează regula de modificarea a parolei la autentificarea în Agentul de Autentificare** dacă dorești ca aplicația Kaspersky Endpoint Security să modifice valoare setării pentru modificarea parolei pentru toate conturile de Agent de autentificare create pe baza contului Microsoft Windows cu numele indicat în câmpul **Cont Windows** cu valoarea pentru setare specificată mai jos.
9. Specifică valoarea pentru setarea de modificare a parolei la autentificarea în Agentul de Autentificare.
10. Bifează caseta de selectare **Modificare setări de autentificare bazată pe certificat** pentru a putea edita setările de autentificare bazate pe un certificat electronic al unui simbol sau card inteligent.

11. Bifează caseta de selectare **Permitere autentificare pe bază de certificat** dacă dorești ca aplicația să solicite utilizatorului să introducă parola pentru simbolul sau cardul inteligent conectat la computer în cursul procesului de autentificare, pentru a accesa unitățile de hard disk criptate.
12. Dacă ai bifat caseta de selectare **Permitere autentificare pe bază de certificat** în pasul anterior, fă clic pe butonul **Răsfoire** și selectează fișierul certificatului electronic al simbolului sau cardului inteligent în fereastra **Selectare fișier de certificat**.
13. Bifează caseta de selectare **Editare descriere comandă** și editează descrierea comenzii dacă dorești ca aplicația Kaspersky Endpoint Security să modifice descrierea comenzii pentru toate conturile de Agent de autentificare create pe baza contului Microsoft Windows cu numele indicat în câmpul **Cont Windows**.
14. Bifează caseta de selectare **Editează regula de acces la autentificare în Agentul de Autentificare** dacă dorești ca aplicația Kaspersky Endpoint Security să modifice regula pentru accesul utilizatorului la dialogul de autentificare pentru toate conturile de Agent de autentificare create pe baza contului Microsoft Windows cu numele indicat în câmpul **Cont Windows**.
15. Specifică regula pentru accesul la dialogul de autentificare în Agentul de Autentificare.
16. În fereastra **Editare cont utilizator**, fă clic pe **OK**.

## Adăugarea unei comenzi pentru ștergerea unui cont de Agent de Autentificare

*Pentru a adăuga o comandă pentru ștergerea unui cont de Agent de Autentificare:*

1. În secțiunea **Setări** din fereastra **Proprietăți: <numele activității de administrare pentru contul de Agent de Autentificare>**, deschide meniul contextual al butonului **Adăugare** și selectează elementul **Comandă de ștergere cont**.  
Apare fereastra **Ștergere cont utilizator**.
2. În câmpul **Cont Windows** din fereastra **Ștergere cont utilizator**, specifică numele contului de utilizator Microsoft Windows care a fost folosit pentru a crea contul de Agent de Autentificare pe care dorești să-l ștergi. Pentru aceasta, tastează manual numele contului sau fă clic pe butonul **Selectare**.
3. Dacă ai introdus manual numele unui cont de utilizator Microsoft Windows, fă clic pe butonul **Permitere** pentru a determina identificatorul de securitate (SID) contului de utilizator.  
Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

Determinarea SID-ului contului de utilizator Microsoft Windows atunci când se adaugă comanda de ștergere pentru un cont de Agent de Autentificare reprezintă un mod convenabil să te asiguri că numele contului de utilizator Microsoft Windows introdus manual este corect. În cazul în care contul de utilizator Microsoft Windows nu există sau aparține unui domeniu care nu este de încredere, activitatea de grup pentru administrarea conturilor de Agent de autentificare se termină cu o eroare.

4. În fereastra **Ștergere cont utilizator**, fă clic pe **OK**.

## Restaurarea acreditărilor pentru contul de Agent de Autentificare

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.

*Pentru a restaura numele de utilizator și parola unui cont de Agent de Autentificare:*

1. Agentul de Autentificare se încarcă pe un computer cu unități de hard disk criptate înainte de încărcarea sistemului de operare. În interfața Agentului de autentificare, apasă pe butonul **Ai uitat parola?** pentru a iniția procesul de restaurare a numelui de utilizator și a parolei pentru un cont de Agent de Autentificare.
2. Urmează instrucțiunile din Agentul de Autentificare pentru a obține unitățile de solicitare pentru restaurarea numelui de utilizator și a parolei pentru contul de Agent de Autentificare.
3. Dictează conținutul blocurilor de solicitare administratorului rețelei LAN, împreună cu numele computerului.
4. Introdu secțiunile din răspunsul la solicitarea de restaurare a numelui de utilizator și parolei pentru contul de Agent de Autentificare care au fost generate și furnizate de către administratorul rețelei LAN.
5. Introdu o parolă nouă pentru contul de Agent de Autentificare și confirm-o.

Numele de utilizator pentru contul de Agent de Autentificare este definit folosind secțiunile din răspunsul la solicitările de restaurare a numelui de utilizator și parolei pentru contul de Agent de Autentificare.

După ce introduci și confirmi noua parolă pentru contul de Agent de Autentificare, parola va fi salvată și ți se va furniza acces la unitățile de hard disk criptate.

# Răspunsul la solicitarea unui utilizator de restaurare a acreditărilor pentru contul de Agent de Autentificare

*Pentru a crea și a trimite secțiunile utilizatorului din răspunsul la solicitarea de nume de utilizator și parolă pentru un cont de Agent de Autentificare:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul utilizatorului care a solicitat restaurarea numelui de utilizator și a parolei unui cont de Agent de Autentificare.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În fila **Dispozitive**, selectează computerul utilizatorului care a solicitat restaurarea numelui de utilizator și a parolei unui cont de Agent de Autentificare și fă clic dreapta pentru a deschide meniul contextual.
5. În meniul contextual, selectează opțiunea **Acordă acces la dispozitive și la date în modul offline**.  
Se deschide fereastra **Acordă acces la dispozitive și la date în modul offline**.
6. În fereastra **Acordă acces la dispozitive și la date în modul offline**, selectează fila **Agent de Autentificare**.
7. În secțiunea **Algoritm de criptare aflat în uz**, selectează tipul de algoritm de criptare.
8. În lista verticală **Cont**, selectează numele contului de Agent de Autentificare creat pentru utilizatorul care solicită recuperarea numelui de utilizator și a parolei unui cont de Agent de Autentificare.
9. În lista verticală **Unitate de hard disk**, selectează unitatea de hard disk criptată pentru care trebuie să recuperezi accesul.
10. În secțiunea **Solicitare utilizator**, introdu blocurile din solicitare dictate de către utilizator.  
Conținutul secțiunilor din răspunsul la solicitarea utilizatorului de recuperare a numelui de utilizator și a parolei unui cont de Agent de Autentificare este afișat în câmpul **Cheie de acces**.
11. Dictează conținutul blocurilor din răspuns utilizatorului.

## Vizualizarea detaliilor de criptare date

Această secțiune descrie cum poți vedea detalii despre criptarea datelor.



## Despre starea de criptare

Atunci când criptarea sau decriptarea este în curs, Kaspersky Endpoint Security transmite informații despre starea parametrilor de criptare aplicați computerelor client de Kaspersky Security Center.

Sunt posibile două valori pentru starea de criptare:

- *Nedefinit de politică.* Nu a fost definită o politică a aplicației Kaspersky Security Center pentru acest computer.
- *Criptare/decriptare în curs.* Criptarea și/sau decriptarea datelor este în curs pe acest computer.
- *Eroare.* A intervenit o eroare în cursul criptării și/sau decriptării datelor pe acest computer.
- *Repornire necesară.* Sistemul de operare trebuie repornit pentru a începe sau a finaliza criptarea sau decriptarea datelor pe acest computer.
- *Conform politicii.* Criptarea și/sau decriptarea datelor pe acest computer a fost finalizată folosind setările de criptare specificate în politica pentru Kaspersky Security Center aplicată computerului.
- *Anulat de utilizator.* Utilizatorul a refuzat să confirme operațiunea de criptare a fișierelor pe unitatea amovibilă.
- *Nu este acceptat.* Funcționalitatea de criptare a datelor nu este disponibilă pe acest computer.

## Vizualizarea stării de criptare

*Pentru a vedea starea de criptare a datelor computerului:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.

Fila **Dispozitive** din spațiul de lucru prezintă proprietățile computerelor din grupul de administrare selectat.

4. În fila **Dispozitive** din spațiul de lucru, defilează până la maximum dreapta baza de defilare.

Coloana **Stare de criptare** afișează starea de criptare a datelor de pe computerele din grupul de administrare selectat. Această stare este prezentată pe baza informațiilor despre criptarea fișierelor pe unitățile locale ale computerului, despre criptarea unităților de hard disk ale computerului și despre criptarea unităților amovibile.

# Vizualizarea statisticilor de criptare în panourile de detalii ale Kaspersky Security Center

*Pentru a vizualiza starea de criptare în panourile de detalii ale Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează nodul **Server de administrare – <Nume computer>**.
3. În spațiul de lucru din dreapta arborelui consolei de administrare, selectează fila **Statistici**.
4. Creează o pagină nouă cu panouri de detalii care conțin statistici de criptare a datelor. Pentru aceasta:
  - a. În fila **Statistici**, fă clic pe butonul **Particularizare vizualizare**.  
Se deschide fereastra **Proprietăți: Statistici**.
  - b. În fereastra **Proprietăți: Statistici**, fă clic pe **Adăugare**.  
Se deschide fereastra **Proprietăți: Pagină nouă**.
  - c. În secțiunea **General** din fereastra **Proprietăți: Pagină nouă**, tastează numele paginii.
  - d. În secțiunea **Panouri de detalii**, fă clic pe butonul **Adăugare**.  
Se deschide fereastra **Panou de detalii nou**.
  - e. În fereastra **Panou de detalii nou** din grupul **Stare protecție**, selectează elementul **Criptare dispozitiv**.
  - f. Fă clic pe **OK**.  
Se deschide fereastra **Proprietăți: Control criptare**.
  - g. Dacă este necesar, editează setările panoului de detalii. Pentru aceasta, folosește secțiunile **Vizualizare** și **Dispozitive** din fereastra **Proprietăți: Criptare dispozitiv**.
  - h. Fă clic pe **OK**.
  - i. Repetă pașii d – h din instrucțiuni, selectând elementul **Criptare unități amovibile** din secțiunea **Stare protecție** din fereastra **Panou de detalii nou**.  
Panourile de detalii adăugate apar în lista **Panouri de detalii** din fereastra **Proprietăți: Pagină nouă**.
  - j. În fereastra **Proprietăți: Pagină nouă**, fă clic pe **OK**.

Numele paginii cu panourile de detalii create în pașii anteriori apare în lista **Pagini** din fereastra **Proprietăți: Statistici**.

k. În fereastra **Proprietăți: Statistici**, fă clic pe **Închidere**.

5. În fila **Statistici**, deschide pagina creată în pașii anteriori din aceste instrucțiuni.

Apar panourile de detalii, prezentând starea de criptare pentru computere și unități amovibile.

## Vizualizarea erorile de criptare fișiere pe unitățile locale ale computerului

*Pentru a vizualiza erorile de criptare fișiere pe unitățile locale ale computerului:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul client pentru care dorești să vezi lista de erori de criptare fișiere.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În fila **Dispozitive**, selectează numele computerului în listă și fă clic dreapta pe el pentru a deschide meniul contextual.
5. Efectuează una dintre următoarele acțiuni:
  - În meniul contextual al computerului, selectează **Protecție**.
  - în meniul contextual al computerului, selectați elementul **Proprietăți**. În fereastra **Proprietăți: <Nume computer>**, selectează secțiunea **Protecție**.
6. În secțiunea **Protecție** din fereastra **Proprietăți: <Nume computer>**, fă clic pe linkul **Vizualizare listă erori de criptare date** pentru a deschide fereastra **Erori criptare date**.

Această fereastră afișează detalii despre erorile de criptare fișiere pe unitățile locale ale computerului. Atunci când o eroare este corectată, Kaspersky Security Center elimină detaliile erorii din fereastra **Erori criptare date**.

## Vizualizarea raportului de criptare a datelor

*Pentru a vizualiza raportul de criptare a datelor:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În nodul **Server de administrare** din arborele consolei de administrare, selectează fila **Rapoarte**.

### 3. Fă clic pe butonul **Creare șablon raport**.

Se lansează Expertul pentru șablon de raport.

### 4. Urmează instrucțiunile din Expertul pentru șablon de raport. În fereastra **Selectează tipul șablonului de raport**, în secțiunea **Altele**, selectează unul dintre elementele următoare:

- **Raportul privind starea criptării dispozitivelor gestionate.**
- **Raportul privind criptarea datelor stocate pe dispozitive.**
- **Raportul privind erorile de criptare.**
- **Raportul Acces blocat la fișiere criptate.**

După ce ai finalizat Expertul de șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Rapoarte**.

### 5. Selectează șablonul de raport creat în pasul anterior al instrucțiunilor.

Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

## Administrarea fișierelor criptate cu funcționalitate de criptare fișiere limitată

Atunci când politica aplicației Kaspersky Security Center se aplică și fișierele sunt apoi criptate, Kaspersky Endpoint Security primește o cheie de criptare necesară pentru accesarea fișierelor criptate. Folosind această cheie de criptare, un utilizator care lucrează sub orice cont de utilizator Windows care era activ în cursul criptării fișierelor poate accesa direct fișierele criptate. Utilizatorii care lucrează sub conturi Windows care erau inactive în cursul criptării fișierelor trebuie să se conecteze la Kaspersky Security Center pentru a accesa fișierele criptate.

Fișierele criptate pot fi inaccesibile în următoarele situații:

- Computerul utilizatorului stochează chei de criptare, dar nu există o conexiune cu aplicația Kaspersky Security Center pentru gestionarea cheilor. În acest caz, utilizatorul trebuie să solicite accesul la fișierele criptate de la administratorul rețelei LAN.

Dacă nu există acces la Kaspersky Security Center, trebuie să procedezi astfel:

- Solicită o cheie de acces pentru accesul la fișiere criptate de pe unitățile de hard disk ale computerului.
- Pentru a accesa fișiere criptate stocate pe unități amovibile, solicită chei de acces separate pentru fișierele criptate de pe fiecare unitate amovibilă.

- Componentele de criptare sunt șterse de pe computerul utilizatorului. În această situație, utilizatorul poate deschide fișiere criptate de pe discuri locale și amovibile, însă conținutul fișierelor respective va apărea criptat.

Utilizatorul poate lucra cu fișiere criptate în următoarele situații:

- Fișierele sunt plasate în [pachete criptate](#) create pe un computer cu aplicația Kaspersky Endpoint Security instalată.
- Fișierele sunt stocate pe unități amovibile pe care a fost permis [modul portabil](#).

## Accesarea fișierelor criptate fără o conexiune la Kaspersky Security Center

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.

*Pentru a accesa fișiere criptate fără a conexiune la Kaspersky Security Center:*

1. Încearcă să accesezi fișierul criptat de care ai nevoie.

Dacă nu există nicio conexiune la Kaspersky Security Center atunci când încerci să accesezi un fișier stocat pe o unitate locală a computerului, Kaspersky Endpoint Security generează un fișier cu o solicitare de acces la toate fișierele criptate care sunt stocate pe unitățile locale ale computerului. Dacă încerci să accesezi un fișier stocat pe o unitate amovibilă, Kaspersky Endpoint Security generează un fișier care solicită accesul la toate fișierele criptate care sunt stocate pe unitatea amovibilă. Se deschide fereastra **Acces la fișier blocat**.

2. Trimite fișierul care conține o solicitare de acces la fișiere criptate administratorului rețelei locale. Pentru aceasta, folosește una dintre metodele următoare:

- Pentru a trimite prin e-mail fișierul care solicită accesul la fișiere criptate administratorului rețelei locale, fă clic pe butonul **Trimitere prin e-mail**.
- Pentru a salva fișierul care solicită accesul la fișiere locale și a-l trimite administratorului rețelei locale printr-o altă metodă, fă clic pe butonul **Salvare**.

3. Obține fișierul cheie pentru accesarea fișierelor criptate care ți-a fost [creat și furnizat](#) de către administratorul rețelei locale.

4. Activează cheia pentru accesarea fișierelor criptate într-unul din modurile următoare:

- În orice program manager de fișiere, selectează fișierul care conține cheia pentru accesul la fișierele criptate. Deschide-l făcând clic dublu pe el.

- Efectuează următoarele acțiuni:

a. Deschide fereastra principală a Kaspersky Endpoint Security.

b. Fă clic pe butonul .

Această acțiune deschide fereastra **Evenimente**.

c. Selectează fila **Stare acces la fișiere și dispozitive** tab.

Fila afișează o listă cu toate solicitările de acces la fișiere criptate.

d. Selectează solicitarea pentru care ai primit fișierul cheie pentru accesarea fișierelor criptate.

e. Pentru a încărca fișierul cheie furnizat pentru accesarea fișierelor criptate, fă clic pe **Răsfoire**.

Se deschide caseta de dialog Microsoft Windows standard **Selectare fișier cheie de acces**.

f. În fereastra standard **Selectare fișier cheie de acces** din Microsoft Windows, selectează fișierul furnizat de administrator, cu extensia .kesdr și cu numele corespunzând numelui de fișier al fișierului de solicitare acces.

g. Fă clic pe butonul **Open** (Deschidere).

h. În fereastra **Evenimente**, fă clic pe **OK**.

Dacă este generat un fișier cu o solicitare de acces la fișiere criptate atunci când încerci să accesezi un fișier stocat pe o unitate locală a computerului, Kaspersky Endpoint Security acordă acces la toate fișierele criptate care sunt stocate pe unitățile locale ale computerului. Dacă este generat un fișier de solicitare acces la fișiere criptate atunci când încerci să accesezi un fișier stocat pe o unitate amovibilă, Kaspersky Endpoint Security acordă acces la toate fișierele criptate stocate pe unitatea amovibilă. Pentru a accesa fișiere criptate stocate pe alte unități amovibile, trebuie să obții un fișier separat cu cheie de acces pentru fiecare unitate amovibilă.

## Acordarea dreptului unui utilizator de a accesa fișiere criptate fără a conexiune la Kaspersky Security Center

*Pentru a acorda dreptul unui utilizator de a accesa fișiere criptate fără o conexiune la Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul utilizatorului care solicită accesul la fișiere criptate.

3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În fila **Dispozitive**, selectează computerul utilizatorului care solicită accesul la fișiere criptate și fă clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectează opțiunea **Acordă acces la dispozitive și la date în modul offline**.  
Se deschide fereastra **Acordă acces la dispozitive și la date în modul offline**.
6. În fereastra **Acordă acces la dispozitive și la date în modul offline**, selectează fila **Criptare**.
7. În fila **Criptare**, fă clic pe butonul **Răsfoire**.  
Se deschide caseta de dialog Microsoft Windows standard **Selectare fișier solicitare acces**.
8. În fereastra **Selectare fișier solicitare acces**, specifică o cale către fișierul de solicitare primit de la utilizator și fă clic pe **Deschis**.  
Kaspersky Security Center generează un fișier cheie pentru accesarea fișierelor criptate.  
Detaliile solicitării utilizatorului sunt afișate în fila **Criptare**.

9. Efectuează una dintre următoarele acțiuni:

- Pentru a trimite utilizatorului prin e-mail fișierul cheie de acces generat, fă clic pe butonul **Trimitere prin e-mail**.
- Pentru a salva fișierul cheie de acces pentru fișiere criptate și a-l trimite utilizatorului printr-o altă metodă, fă clic pe butonul **Salvare**.

## Editarea șabloanelor de mesaje pentru acces la fișiere criptate

*Pentru a edita șabloanele de mesaje pentru acces la fișiere criptate:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să editezi șabloanele de mesaje pentru solicitarea accesului la fișiere criptate.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.

- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

6. În secțiunea **Criptare date**, selectează subsecțiunea **Setări de criptare comune**.

7. În secțiunea **Șabloane**, fă clic pe butonul **Șabloane**.

Se deschide fereastra **Șabloane**.

8. Efectuează următoarele acțiuni:

- Dacă dorești să editezi șablonul pentru mesajul utilizatorului, selectează fila **Mesajul utilizatorului**. Fereastra **Acces refuzat la fișier** se deschide atunci când utilizatorul încearcă să acceseze un fișier criptat și nu există pe computer care nicio cheie disponibilă pentru accesul la fișiere criptate. Fă clic pe butonul **Trimitere prin e-mail** în fereastra **Acces refuzat la fișier** pentru a crea un mesaj al utilizatorului. Acest mesaj este trimis administratorului rețelei LAN, împreună cu fișierul prin care se solicită accesul la fișiere criptate.
- Dacă dorești să editezi șablonul pentru mesajul administratorului, selectează fila **Mesajul administratorului**. Acest mesaj este creat automat atunci când se face clic pe butonul **Trimitere prin e-mail** în fereastra **Acordare acces la fișiere criptate** și este trimis utilizatorului după ce acestuia i se acordă acces la fișiere criptate.

9. Editează șabloanele de mesaje.

Poți folosi butonul **Implicit** și lista verticală **Variabilă**.

10. Fă clic pe **OK**.

11. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.

## Lucrul cu dispozitive criptate atunci când nu există acces la acestea

### Obținerea accesului la dispozitive criptate

Este posibil ca un utilizator să trebuiască să solicite acces la dispozitive criptate în următoarele cazuri:

- Unitatea de hard disk a fost criptată pe alt computer.
- Cheia de criptare pentru un dispozitiv nu este pe computer (de exemplu, la prima încercare de a accesa a unității amovibile criptate pe computer) și computerul nu este conectat la Kaspersky Security Center.



După ce utilizatorul a aplicat cheia de acces dispozitivului criptat, Kaspersky Endpoint Security salvează cheia de criptare pe computerul utilizatorului și permite accesul la acest dispozitiv la încercările de accesare ulterioare chiar dacă nu există conexiune la Kaspersky Security Center.

Accesul la dispozitive criptate poate fi obținut după cum urmează:

1. Utilizatorul [folosește interfața aplicației Kaspersky Endpoint Security pentru a crea un fișier de solicitare acces](#) cu extensia kesdc și-l trimite administratorului rețelei LAN a companiei.
2. Administratorul [utilizează Consola de administrare Kaspersky Security Center pentru a crea un fișier cheie de acces](#) cu extensia kesdr și-l trimite utilizatorului.
3. Utilizatorul [aplică cheia de acces](#).

## Restaurarea datelor pe dispozitive criptate

Un utilizator poate folosi [Utilitarul de restaurare pentru dispozitive criptate](#) (denumit în continuare Utilitarul de restaurare) pentru a lucra cu dispozitive criptate. Acest lucru este necesar în următoarele cazuri:

- Procedura pentru utilizarea unei chei de acces pentru obținerea accesului nu s-a finalizat cu succes.
- Componentele de criptare nu au fost instalate pe computer cu dispozitivul criptat.

Datele necesare pentru restaurarea accesului la dispozitive criptate utilizându-se Utilitarul de restaurare sunt rezidente de câțva timp în memoria computerului utilizatorului în formă necriptată. Pentru a reduce riscul de acces neautorizat la astfel de date, te sfătuim să restaurezi accesul la dispozitive criptate pe dispozitive de încredere.

Datele de pe dispozitive criptate pot fi restaurate după cum urmează:

1. Utilizatorul [folosește Utilitarul de restaurare pentru a crea un fișier de solicitare acces](#) cu extensia fdertc și-l trimite administratorului rețelei LAN a companiei.
2. Administratorul [utilizează Consola de administrare Kaspersky Security Center pentru a crea un fișier cheie de acces](#) cu extensia fdertr și-l trimite utilizatorului.
3. Utilizatorul [aplică cheia de acces](#).

Pentru a restaura date pe unități de hard disk de sistem criptate, utilizatorul poate, de asemenea, să specifice acreditările pentru contul de Agent de Autentificare în Utilitarul de restaurare. Dacă metadatele contului de Agent de Autentificare au fost corupte, utilizatorul trebuie să finalizeze procedura de restaurare utilizând fișierul de solicitare acces.

Înainte de a restaura date pe dispozitive criptate, este recomandabil să revoci politica de criptare Kaspersky Security Center pe computerul unde trebuie efectuată această operațiune. Aceasta împiedică unitatea să fie criptată din nou.

## Obținerea accesului la dispozitive criptate prin intermediul interfeței aplicației

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.


*Pentru a obține acces la dispozitive criptate prin intermediul interfeței aplicației:*

1. Încearcă să accesezi dispozitivul criptat de care ai nevoie.


Se deschide fereastra **Accesul la date este blocat**.

2. Trimite administratorului rețelei LAN a companiei fișierului de solicitare acces cu extensia kesdc pentru fișierul criptat. Pentru aceasta, folosește una dintre metodele următoare:

- Pentru a trimite prin e-mail administratorului rețelei LAN a companiei fișierul de solicitare acces generat pentru dispozitivul criptat, fă clic pe butonul **Trimitere prin e-mail**.
- Pentru a salva fișierul de solicitare acces pentru dispozitivul criptat și a-l trimite administratorului rețelei LAN a companiei printr-o altă metodă, fă clic pe butonul **Salvare**.

Dacă ai închis fereastra **Accesul la date este blocat** fără a salva fișierul de solicitare acces sau fără trimiterea acestuia administratorului rețelei LAN a companiei, poți face acest lucru oricând în fereastra **Evenimente** din fila **Stare acces la fișiere și dispozitive**. Pentru a deschide această fereastră, fă clic pe butonul  în fereastra principală a aplicației.

3. Obține și salvează fișierul cheie de acces pentru dispozitivul criptat care a fost [creat și furnizat](#) de administratorul rețelei LAN a companiei.
4. Utilizează una dintre următoarele metode pentru a aplica cheia de acces pentru accesarea dispozitivului criptat:

- În orice manager de fișiere, găsește fișierul cheie de acces pentru dispozitivul criptat și fă dublu clic pe acesta pentru a-l deschide.
- Efectuează următoarele acțiuni:
  - a. Deschide fereastra principală a Kaspersky Endpoint Security.
  - b. Fă clic pe butonul  pentru a deschide fereastra **Evenimente**.
  - c. Selectează fila **Stare acces la fișiere și dispozitive** tab.

Fila afișează o listă cu toate solicitările de acces la fișiere și dispozitive criptate.
  - d. Selectează numărul solicitării pentru care ai primit fișierul cheie de acces pentru accesarea dispozitivului criptat.
  - e. Pentru a încărca fișierul cheie de acces primit pentru accesarea dispozitivului criptat, fă clic pe **Răsfoire**.

Se deschide caseta de dialog Microsoft Windows standard **Selectare fișier cheie de acces**.
  - f. În fereastra standard **Selectare fișier cheie de acces** din Microsoft Windows, selectează fișierul furnizat de administrator, cu extensia kesdr și cu numele de fișier corespunzător fișierului de solicitare acces pentru dispozitivul criptat.
  - g. Fă clic pe butonul **Open** (Deschidere).
  - h. În fereastra **Stare acces la fișiere și dispozitive**, fă clic pe **OK**.

Kaspersky Endpoint Security va acorda acces la dispozitivul criptat.

## Acordarea accesului utilizatorului la dispozitive criptate

*Pentru a acorda acces unui utilizator la un dispozitiv criptat:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul utilizatorului care solicită accesul la dispozitivul criptat.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În fila **Dispozitive**, selectează computerul utilizatorului care solicită acces la dispozitivul criptat și fă clic dreapta pe el pentru a deschide meniul contextual.

5. În meniul contextual, selectează opțiunea **Acordă acces la dispozitive și la date în modul offline**.

Se deschide fereastra **Acordă acces la dispozitive și la date în modul offline**.

6. În fereastra **Acordă acces la dispozitive și la date în modul offline**, selectează fila **Criptare**.

7. În fila **Criptare**, fă clic pe butonul **Răsfoire**.

Se deschide caseta de dialog Microsoft Windows standard **Selectare fișier solicitare acces**.

8. În fereastra **Selectare fișier solicitare acces**, introdu calea către fișierul de solicitare cu extensia kesdc pe care l-ai primit de la utilizator.

9. Fă clic pe butonul **Open** (Deschidere).

Kaspersky Security Center generează un fișier de cheie de acces la dispozitivul criptat cu extensia kesdr. Detaliile solicitării utilizatorului sunt afișate în fila **Criptare**.

10. Efectuează una dintre următoarele acțiuni:

- Pentru a trimite utilizatorului prin e-mail fișierul cheie de acces generat, fă clic pe butonul **Trimitere prin e-mail**.
- Pentru a salva fișierul cheie de acces pentru dispozitivul criptat și a-l trimite utilizatorului printr-o altă metodă, fă clic pe butonul **Salvare**.

## Furnizarea unei chei de recuperare pentru unități de hard disk criptate cu BitLocker

*Pentru a trimite unui utilizator o cheie de recuperare pentru o unitate de hard disk de sistem care a fost criptată folosind BitLocker:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul utilizatorului care solicită accesul la unitatea criptată.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În fila **Dispozitive**, selectează computerul care aparține utilizatorului care solicită accesul la unitatea criptată.
5. Fă clic dreapta pentru a deschide meniul contextual și selectează **Acordă acces la dispozitive și la date în modul offline**.

Se deschide fereastra **Acordă acces la dispozitive și la date în modul offline**.

6. În fereastra **Acordă acces la dispozitive și la date în modul offline**, selectează fila **Acces la o unitate de sistem protejată de BitLocker**.
7. Solicită utilizatorului ID-ul cheii de recuperare, indicat în fereastra de introducere a parolei BitLocker, și compară-l cu ID-ul din câmpul **ID cheie de recuperare**.

Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea de sistem specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

8. Trimite utilizatorului cheia indicată în câmpul **Cheie de recuperare**.

*Pentru a trimite unui utilizator o cheie de recuperare pentru o unitate de hard disk non-sistem care a fost criptată folosind BitLocker:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectează directorul **Suplimentar** → **criptare și protecție date** → **Dispozitive criptate**.  
Spațiul de lucru afișează o listă de dispozitive criptate.
3. În spațiul de lucru, selectează dispozitivul criptat la care trebuie să restaurezi accesul.
4. Fă clic dreapta pentru a afișa meniul contextual și selectează **Obține cheie de acces la dispozitivul criptat specificat**.  
Se deschide fereastra **Restaurare acces la o unitate criptată cu BitLocker**.
5. Solicită utilizatorului ID-ul cheii de recuperare, indicat în fereastra de introducere a parolei BitLocker, și compară-l cu ID-ul din câmpul **ID cheie de recuperare**.

Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

6. Trimite utilizatorului cheia indicată în câmpul **Cheie de recuperare**.

## Crearea fișierului executabil fdert.exe al utilitarului Restaurare

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.


*Pentru a crea fișierul executabil fdert.exe al utilitarului Restaurare:*

1. Deschide [fereastra principală a aplicației](#).
2. Fă clic pe butonul  în colțul stânga jos al ferestrei principale a aplicației, pentru a deschide fereastra **Asistență**.
3. În fereastra **Asistență**, fă clic pe butonul **Restaurarea dispozitiv criptat**.  
Se lansează Utilitarul de restaurare pentru dispozitive criptate.
4. Fă clic pe butonul **Creare Utilitar de restaurare independent** în fereastra utilitarului Restaurare.  
Se deschide fereastra **Se creează un Utilitar de restaurare independent**.
5. În fereastra **Salvare în**, tastează manual calea către directorul pentru salvarea fișierului executabil al utilitarului Restaurare sau fă clic pe butonul **Răsfoire**.
6. Fă clic pe **OK** în fereastra **Se creează un Utilitar de restaurare independent**.  
Fișierul executabil al Utilitarului de restaurare (fdert.exe) este salvat în directorul selectat.

## Restaurarea datelor pe dispozitivele criptate folosind Utilitarul de restaurare

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.

*Pentru a restaura accesul la un dispozitiv criptat folosind Utilitarul de restaurare:*

1. Execută utilitarul Restaurare într-unul din modurile următoare:
  - Fă clic pe butonul  în fereastra principală a Kaspersky Endpoint Security pentru a deschide fereastra **Asistență** și fă clic pe butonul **Restaurarea dispozitiv criptat**.
  - Execută fișierul executabil fdert.exe al utilitarului Restaurare. [Acest fișier este creat de Kaspersky Endpoint Security](#).
2. În fereastra Utilitar Restaurare, în lista verticală **Selectare dispozitiv**, selectează un dispozitiv criptat la care dorești să restaurezi accesul.
3. Fă clic pe butonul **Scanare** pentru a permite utilitarului să definească acțiunile care trebuie efectuate asupra dispozitivului: acesta trebuie deblocat sau decriptat.

În cazul în care computerul are acces la funcționalitatea de criptare Kaspersky Endpoint Security, Utilitarul de restaurare îți solicită să deblochezi dispozitivul. Deblocarea unui dispozitiv nu este sinonimă cu decriptarea lui, dar dispozitivul devine accesibil direct ca urmare a acțiunii de deblocare. În cazul în care computerul nu are acces la funcționalitatea de criptare Kaspersky Endpoint Security, Utilitarul de restaurare îți solicită să decriptezi dispozitivul.

4. Fă clic pe butonul **Remediere MBR** dacă diagnosticarea unității de hard disk de sistem criptat a returnat un mesaj despre probleme cu înregistrarea master boot record (MBR) a dispozitivului.

Remedierea înregistrării master boot record a dispozitivului poate accelera procesul de colectare a informațiilor necesare pentru deblocarea sau decriptarea dispozitivului.

5. Fă clic pe butonul **Deblocare** sau **Decriptare** în funcție de rezultatele diagnosticării.

Se deschide fereastra **Setări pentru deblocare dispozitiv/Setări decriptare dispozitiv**.

6. Dacă dorești să restaurezi date utilizând un cont Agent de Autentificare:

- a. Selectează opțiunea **Utilizare parametri de cont pentru Agentul de Autentificare**.

- b. În câmpurile **Nume** și **Parolă**, specifică acreditările pentru contul Agent de Autentificare.

Această metodă este posibilă numai la restaurarea datelor pe o unitate de hard disk de sistem. Dacă unitatea de hard disk de sistem a fost coruptă și datele contului Agent de Autentificare s-au pierdut, trebuie să obții o cheie de acces de la administratorul rețelei LAN a companiei pentru a restaura date pe un dispozitiv criptat.

7. Dacă dorești să utilizezi o cheie de acces pentru a restaura date:

- a. Selectează opțiunea **Specificare manuală cheie de acces pentru dispozitiv**.

- b. Fă clic pe butonul **Primire cheie de acces**.

- c. Se deschide fereastra **Primire cheie de acces pentru dispozitiv**.

- d. Fă clic pe butonul **Salvare** și selectează directorul în care se salvează fișierul de solicitare acces cu extensia fdertc.

- e. Trimite fișierul de solicitare acces administratorului rețelei LAN a companiei.

Nu închide fereastra **Primire cheie de acces pentru dispozitiv** până când nu primești cheia de acces. Atunci când se deschide din nou această fereastră, nu mai poți aplica cheia de acces creată anterior de către administrator.

- f. Obține și salvează fișierul cheie de acces [creată și furnizată](#) de către administratorul rețelei LAN a companiei.

g. Fă clic pe butonul **Încărcare** și selectează fișierul cheie de acces cu extensia fdertr în fereastra care se deschide.

8. Dacă decriptezi un dispozitiv, trebuie să specifici și celelalte setări de decriptare în fereastra **Setări decriptare dispozitiv**. Pentru aceasta:

- Specifică zona de decriptat:
  - Dacă dorești să decriptezi întregul dispozitiv, selectează opțiunea **Decriptare întregul dispozitiv**.
  - Dacă dorești să decriptezi o parte din datele d pe un dispozitiv, selectează opțiunea **Decriptare zone individuale din dispozitiv** și utilizează câmpurile **Început** și **Terminare** pentru a specifica limitele zonei d decriptat.
- Selectează locația pentru scrierea datelor decriptate:
  - Dacă dorești rescrierea datelor de pe dispozitivul original cu datele decriptate, debifează caseta de selectare **Salvare date în fișier după decriptare**.
  - Dacă dorești să salvezi datele decriptate separat de datele criptate originale, bifează caseta de selectare **Salvare date în fișier după decriptare** și utilizează butonul **Răsfoire** pentru a furniza calea către locația d salvare a datelor.

9. Fă clic pe **OK**.

Începe procesul de deblocare/decriptare.

## Răspunsul la solicitarea unui utilizator de a restaura date pe dispozitive criptate

*Pentru a crea și a furniza unui utilizator un fișier cheie pentru accesul la un dispozitiv criptat:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectează directorul **Suplimentar** → **criptare și protecție date** → **Dispozitive criptate**.
3. În spațiul de lucru, selectează dispozitivul criptat pentru care dorești să creezi un fișier cheie de acces și, în meniul contextual al dispozitivului, selectează **Obține cheie de acces la dispozitivul criptat specificat**.



Dacă nu ești sigur pentru ce computer a fost generat fișierul de solicitare acces, în arborele consolei de administrare, selectează directorul **Suplimentar** → **Criptare și protecție date** și, în spațiul de lucru, fă clic pe linkul **Obține cheia de criptare a dispozitivului**.

Se deschide fereastra **Permite accesul la dispozitiv**.

4. Selectează algoritmul de criptare în uz. Pentru aceasta, selectează una dintre următoarele opțiuni:

- **AES256**, în cazul în care Kaspersky Endpoint Security a fost instalat dintr-un pachet de distribuție amplasat în directorul aes256 de pe computerul pe care a fost criptat dispozitivul;
- **AES56**, în cazul în care Kaspersky Endpoint Security a fost instalat dintr-un pachet de distribuție amplasat în directorul aes56 de pe computerul pe care a fost criptat dispozitivul;

5. Fă clic pe butonul **Răsfoire**.

Se deschide caseta de dialog Microsoft Windows standard **Selectare fișier solicitare acces**.

6. În fereastra **Selectare fișier solicitare acces**, introdu calea către fișierul de solicitare cu extensia fdertc pe care l-ai primit de la utilizator.

7. Fă clic pe butonul **Open** (Deschidere).

Kaspersky Security Center generează un fișier cheie de acces cu extensia fdertr pentru accesarea dispozitivului criptat.

8. Efectuează una dintre următoarele acțiuni:

- Pentru a trimite utilizatorului prin e-mail fișierul cheie de acces generat, fă clic pe butonul **Trimitere prin e-mail**.
- Pentru a salva fișierul cheie de acces pentru dispozitivul criptat și a-l trimite utilizatorului printr-o altă metodă, fă clic pe butonul **Salvare**.

## Restaurarea accesului la date criptate după o eroare de sistem

Poți restabili accesul la date după o eroare de sistem numai pentru File Level Encryption (FLE). Nu poți restaura accesul la date dacă se folosește Full Disk Encryption (FDE).

*Pentru a restaura accesul la date criptate după o eroare de sistem:*

1. Reinstalează sistemul de operare, fără a formata unitatea de hard disk.
2. [Instalează Kaspersky Endpoint Security](#).
3. Stabiliți o conexiune între computer și Serverul de administrare Kaspersky Security Center care controlează computerul în timpul criptării datelor.

Accesul la datele criptate va fi acordat în aceleași condiții care erau valabile înainte de eroarea sistemului de operare.


## Crearea unui disc de recuperare pentru sistemul de operare

Discul de recuperare pentru sistemul de operare poate fi util atunci când nu se poate accesa o unitate de hard disk criptată dintr-un motiv oarecare sau atunci când sistemul de operare nu se poate încărca.

Poți încărca o imagine a sistemului de operare Windows folosind discul de recuperare și poți restaura accesul la unitatea de hard disk criptată folosind utilitarul Restaurare inclus în imaginea sistemului de operare.

*Pentru a crea un disc de recuperare pentru sistemul de operare:*

1. [Creează un fișier executabil pentru Utilitarul de restaurare pentru dispozitive criptate](#).
2. Creează o imagine particularizată a mediului pre-boot Windows. Atunci când creezi o imagine particularizată a mediului pre-boot Windows, adaugă la imagine fișierul executabil al utilitarului Restaurare.
3. Salvează imaginea particularizată a mediului pre-instalare Windows pe un mediu bootabil, cum ar fi un CD sau o unitate amovibilă.

Consultă fișierele de ajutor Microsoft pentru instrucțiuni referitoare la crearea unei imagini particularizate a mediului pre-boot Windows (de exemplu, în acest [resurse Microsoft TechNet](#) ).

## Protecție rețea

Această secțiune conține informații despre monitorizarea traficului de rețea și instrucțiuni despre configurarea setărilor porturilor de rețea monitorizate.

## Despre Protecție rețea

În cursul funcționării Kaspersky Endpoint Security, unele component cum ar fi [Antivirus pentru e-mail](#), [Antivirus pentru Web](#) și [Antivirus MI](#) monitorizează fluxurile de date care sunt transmise prin diferite protocoale specifice și care trec prin porturi TCP și UDP specifice deschise pe computerul tău. De exemplu, Antivirusul pentru e-mail scanează date transmise prin SMTP, în timp ce Antivirusul pentru Web scanează date transmise prin protocoalele HTTP și FTP.

Kaspersky Endpoint Security împarte porturile TCP și UDP ale sistemului de operare în mai multe grupuri, în funcție de probabilitatea ca ele să fie compromise. Unele porturi de rețea sunt rezervate pentru servicii care pot fi vulnerabile. Ești sfătuit să monitorizezi aceste porturi cu mai multă atenție, deoarece probabilitatea ca ele să fie atacate este mai mare. Dacă utilizezi servicii non-standard care se bazează pe porturi de rețea non-standard, aceste porturi de rețea pot și ele să fie vizate de un computer atacator. Poți specifica o listă de porturi de rețea și o listă de aplicații care solicită acces la rețea. Aceste porturi și aplicații apoi beneficiază de atenție specială din partea componentelor Antivirus pentru e-mail, Antivirus pentru Web și Antivirus pentru MI, atunci când acestea monitorizează traficul de rețea.

## Configurarea setărilor pentru monitorizarea traficului de rețea

Poți efectua următoarele acțiuni pentru a configura setările pentru monitorizarea traficului de rețea:

- Activarea monitorizării tuturor porturilor de rețea.
- Crearea unei liste de porturi de rețea monitorizate.
- Crearea unei liste de aplicații pentru care sunt monitorizate toate porturile de rețea.

## Activarea monitorizării tuturor porturilor de rețea

*Pentru a activa monitorizarea tuturor porturilor de rețea:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Protecție antivirus**.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Porturi monitorizate**, selectează **Monitorizare toate porturile de rețea**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Crearea unei liste de porturi de rețea monitorizate

*Pentru a crea o listă de porturi de rețea monitorizate:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, selectează secțiunea **Protecție antivirus**.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Porturi monitorizate**, selectează **Monitorizare numai porturi selectate**.

4. Fă clic pe butonul **Setări**.

Se deschide fereastra **Porturi rețea**. Fereastra **Porturi rețea** afișează o listă de porturi de rețea care, în mod normal, sunt utilizate pentru transmiterea e-mailurilor și a traficului de rețea.

Această listă de porturi de rețea este inclusă în pachetul Kaspersky Endpoint Security.

5. În lista de porturi de rețea poți efectua următoarele acțiuni:

- Bifează casetele de selectare de lângă porturile de rețea pe care dorești să le incluzi în lista de porturi de rețea monitorizate.

Casetele de selectare de lângă toate porturile de rețea listate în fereastra **Porturi rețea** sunt bifate în mod implicit.

- Debifează casetele de selectare de lângă porturile de rețea pe care dorești să le excluzi din lista de porturi de rețea monitorizate.

6. Dacă un port de rețea nu este afișat în lista de porturi de rețea, adaugă-l astfel:

a. Sub lista de porturi de rețea, fă clic pe linkul **Adăugare** pentru a deschide fereastra **Port rețea**.

b. Introdu numărul portului de rețea în câmpul **Port**.

c. Introdu numele portului de rețea în câmpul **Descriere**.

d. Fă clic pe **OK**.

Fereastra **Port rețea** se închide. Portul de rețea adăugat recent se afișează la sfârșitul listei de porturi de rețea.

7. În fereastra **Porturi rețea**, fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Atunci când protocolul FTP se execută în modul pasiv, conexiunea poate fi stabilită printr-un port de rețea aleatoriu, care nu este adăugat în lista de porturi de rețea monitorizate. Pentru a proteja astfel de conexiuni, bifează caseta de selectare **Monitorizare toate porturile de rețea** în secțiunea **Porturi monitorizate** sau [configurează monitorizarea tuturor porturilor pentru aplicații](#) care stabilesc conexiuni FTP.

# Crearea unei liste de aplicații pentru care sunt monitorizate toate porturile de rețea

Poți crea o listă de aplicații pentru care Kaspersky Endpoint Security monitorizează toate porturile de rețea.

Recomandăm includerea aplicațiilor care primesc sau transmit date prin protocolul FTP din lista de aplicații pentru care Kaspersky Endpoint Security monitorizează toate porturile de rețea.

*Pentru a crea o listă de aplicații pentru care sunt monitorizate toate porturile de rețea:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, selectează secțiunea **Protecție antivirus**.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Porturi monitorizate**, selectează **Monitorizare numai porturi selectate**.

4. Fă clic pe butonul **Setări**.

Se deschide fereastra **Porturi rețea**.

5. Bifează caseta de selectare **Monitorizare toate porturile pentru aplicații specificate**.

6. În lista de aplicații de sub caseta de selectare **Monitorizare toate porturile pentru aplicații specificate**, efectuează următoarele:

- Bifează casetele de selectare din dreptul numelor aplicațiilor pentru care dorești să monitorizezi toate porturile de rețea.

Casetele de selectare de lângă toate aplicațiile listate în fereastra **Porturi rețea** sunt bifate în mod implicit.

- Debifează casetele de selectare din dreptul numelor aplicațiilor pentru care nu dorești să monitorizezi toate porturile de rețea.

7. Dacă o aplicație nu este inclusă în lista de aplicații, adaug-o după cum urmează:

a. Fă clic pe linkul **Adăugare** din lista de aplicații și deschide meniul contextual.

b. În meniul contextual, selectează modul în care să adaugi aplicația în lista de aplicații:

- Pentru a selecta o aplicație din lista aplicațiilor instalate pe computer, selectează comanda **Aplicații**. Se deschide fereastra **Selectare aplicația**, care permite specificarea numelui aplicației.
- Pentru a specifica locația fișierului executabil al aplicației, selectează comanda **Răsfoire**. Se deschide fereastra **Open (Deschidere)** standard din Microsoft Windows, care permite specificarea numelui fișierului executabil al aplicației.

După ce selectezi aplicația, se deschide fereastra **Aplicație**.

c. În câmpul **Nume**, introdu numele aplicației selectate.

d. Fă clic pe **OK**.

Fereastra **Aplicație** se închide. Aplicația pe care ai adăugat-o apare la sfârșitul listei de aplicații.

8. În fereastra **Porturi rețea**, fă clic pe **OK**.

9. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Actualizarea bazelor de date și modulelor aplicației

Această secțiune conține informații despre actualizările bazelor de date și modulelor aplicației (denumite și „actualizări”) și instrucțiuni despre modul de configurare a setărilor pentru actualizare.

## Despre actualizarea bazelor de date și modulelor aplicației

Actualizarea bazelor de date și modulelor aplicației Kaspersky Endpoint Security asigură o protecție actualizată pe computer. Zilnic apar în întreaga lume viruși și alte tipuri de programe malware noi. Bazele de date Kaspersky Endpoint Security conțin informații despre amenințări și despre modurile de neutralizare a acestora. Pentru a detecta rapid amenințările, este esențial să actualizezi în mod regulat bazele de date și modulele aplicației.

Actualizările regulate necesită o licență activă. Dacă nu există nicio licență curentă, vei avea posibilitatea să efectuezi doar o singură actualizare.

Sursa principală de actualizare a aplicației Kaspersky Endpoint Security o reprezintă serverele de actualizare Kaspersky.

Computerul trebuie să fie conectat la Internet pentru a descărca cu succes pachetul de actualizare de pe serverele de actualizare Kaspersky. În mod implicit, setările de conectare la Internet sunt stabilite automat. Dacă utilizezi un server proxy, trebuie să [ajustezi setările de conectare](#).

La efectuarea unei actualizări, pe computer sunt descărcate și instalate următoarele obiecte:

- Baze de date Kaspersky Endpoint Security. Protecția computerului este furnizată folosind baze de date care conțin semnături de viruși și alte amenințări și informații despre modalitățile pentru neutralizarea acestora. Componentele protecției utilizează aceste informații la căutarea de fișiere infectate pe computer și la neutralizarea acestora. Bazele de date sunt actualizate constant cu înregistrări de amenințări noi și metode pentru contracararea lor. Prin urmare, îți recomandăm să actualizezi bazele de date regulat.

Pe lângă bazele de date Kaspersky Endpoint Security, sunt actualizate și driverele de rețea care le permit componentelor aplicației să intercepteze traficul de rețea.

- Modulele aplicației. Pe lângă bazele de date Kaspersky Endpoint Security, poți actualiza și modulele aplicației. Actualizarea modulelor aplicației remediază vulnerabilitățile din Kaspersky Endpoint Security, adaugă funcții noi și îmbunătățește funcțiile existente.

În timpul actualizării, modulele și bazele de date ale aplicației de pe computer sunt comparate cu versiunile lor actualizate din sursa de actualizare. Dacă bazele de date și modulele actuale ale aplicației diferă de versiunile lor actualizate, porțiunea lipsă care să regăsește în actualizări este instalată pe computer.

Fișierele de ajutor contextual pentru aplicație pot fi actualizate odată cu actualizările modulelor aplicației.

Dacă bazele de date sunt neactuale, este posibil ca dimensiunea pachetului de actualizare să fie mare (până la câteva zeci de MO), fapt care poate cauza sporirea traficului din Internet.

Informațiile despre starea actuală a bazelor de date Kaspersky Endpoint Security pot fi accesate făcând clic pe linkul **Actualizare** din secțiunea **Activități** a filei **Protecție și control** a [ferestrei principale a aplicației](#).

Informațiile despre rezultatele actualizărilor și despre toate evenimentele care apar în timpul funcționării activității de actualizare sunt înregistrate în [Raportul Kaspersky Endpoint Security](#).

## Despre sursele de actualizare

O *sursă de actualizare* este o resursă care conține actualizări pentru bazele de date și modulele aplicației Kaspersky Endpoint Security.

Sursele de actualizare includ serverul Kaspersky Security Center, serverele de actualizare ale Kaspersky și directoare de rețea sau locale.

# Configurarea setărilor pentru actualizare

Se pot efectua următoarele acțiuni pentru configurarea setărilor de actualizare:

- Adăugare a unor surse de actualizare noi.

Lista implicită de surse de actualizare include Kaspersky Security Center și servere de actualizare ale Kaspersky. Poți adăuga la listă alte surse de actualizare. Poți specifica drept surse de actualizare servere HTTP/FTP și directoare partajate.

Dacă mai multe resurse sunt selectate drept surse de actualizare, Kaspersky Endpoint Security încearcă să se conecteze la ele pe rând, începând cu prima din listă și efectuează acțiunea de actualizare preluând pachetul de actualizare de la prima sursă disponibilă.

Dacă selectezi ca sursă de actualizare o resursă din afara rețelei LAN, pentru a efectua o actualizare, trebuie să dispui de o conexiune la Internet.

- Selectați regiunea serverului de actualizare al Kaspersky.

Dacă utilizezi servere de actualizare ale Kaspersky drept surse de actualizare, poți selecta locația serverului de actualizare al Kaspersky folosit pentru descărcarea pachetului de actualizare. Servere de actualizare ale Kaspersky se găsesc în mai multe țări. Utilizarea celui mai apropiat server de actualizare Kaspersky ajută la reducerea timpului petrecut pentru preluarea pachetului de actualizare.

În mod implicit, aplicația utilizează informații despre regiunea actuală din registrul sistemului de operare.

- Configurează actualizarea aplicației Kaspersky Endpoint Security dintr-un director partajat.

Pentru a reduce traficul pe Internet, poți configura actualizări Kaspersky Endpoint Security astfel încât computerele din rețeaua ta LAN să primească actualizări dintr-un director partajat. În acest scop, unul din computerele aflate în rețeaua ta LAN primește un pachet de actualizare de la serverul Kaspersky Security Center sau de la servere de actualizare Kaspersky și apoi copiază pachetul de actualizare preluat într-un director partajat. După aceea, celelalte computere din rețeaua LAN pot primi pachetul de actualizare din acest director partajat.

- Selectează modul de executare a activității de actualizare.

Dacă nu se poate executa acțiunea de actualizare dintr-un anumit motiv (de exemplu, computerul nu este pornit la momentul respectiv), poți configura activitatea omisă pentru pornire automată atunci când este posibil.

Poți amâna lansarea activității de actualizare după pornirea aplicației, dacă selectezi modul de executare **După planificare** pentru activitatea de actualizare și dacă ora de pornire a Kaspersky Endpoint Security corespunde planificării pornirii activității de actualizare. Activitatea de actualizare se poate executa numai după scurgerea intervalului de timp specificat de la pornirea aplicației Kaspersky Endpoint Security.



- Configurează activitatea de actualizare pentru executare pe baza drepturilor unui alt cont de utilizator.

## Adăugarea unei surse de actualizare

*Pentru a adăuga o sursă de actualizare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Mod executare și sursă actualizare**, fă clic pe butonul **Sursă actualizare**.  
Această acțiune deschide fila **Sursă** din fereastra **Actualizare**.
4. În fila **Sursă**, fă clic pe butonul **Adăugare**.  
Se deschide fereastra **Selectare sursă actualizare**.
5. În fereastra **Selectare sursă actualizare**, selectează directorul care conține pachetul de actualizare sau introdu calea completă către director în câmpul **Sursă**.
6. Fă clic pe **OK**.
7. În fereastra **Actualizare**, fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Selectarea regiunii pentru serverul de actualizare

*Pentru a selecta regiunea pentru serverul de actualizare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Mod executare și sursă actualizare**, fă clic pe butonul **Sursă actualizare**.  
Această acțiune deschide fila **Sursă** din fereastra **Actualizare**.
4. În fila **Sursă**, în secțiunea **Setări regionale**, alege **Selectare din listă**.
5. În lista verticală, selectează țara în funcție de locul în care te afli.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea actualizărilor dintr-un director partajat

Configurarea actualizărilor aplicației Kaspersky Endpoint Security dintr-un director partajat presupune următorii pași:

1. Permitea copierii unui pachet de actualizare într-un director partajat de pe unul dintre computerele din rețeaua locală.
2. Configurarea actualizărilor aplicației Kaspersky Endpoint Security din directorul partajat specificat pe celelalte computere din rețeaua locală.

*Pentru a permite copierea pachetului de actualizare în directorul partajat:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În fila **Suplimentar**, bifează caseta de selectare **Copiere actualizări în folder**.
4. Precizează calea către directorul partajat în care va fi amplasat pachetul de actualizare. Poți face acest lucru în următoarele două moduri:
  - Introdu calea către directorul partajat în câmpul de sub caseta de selectare **Copiere actualizări în folder**.
  - Fă clic pe butonul **Răsfoire**. Apoi, în fereastra **Selectare director** care se deschide, selectează directorul necesar și fă clic pe **OK**.
5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

*Pentru a configura actualizarea aplicației Kaspersky Endpoint Security dintr-un director partajat:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Mod executare și sursă actualizare**, fă clic pe butonul **Sursă actualizare**.  
Această acțiune deschide fila **Sursă** din fereastra **Actualizare**.

4. În fila **Sursă**, fă clic pe butonul **Adăugare**.

Se deschide fereastra **Selectare sursă actualizare**.

5. În fereastra **Selectare sursă actualizare**, selectează directorul partajat care conține pachetul de actualizare sau introdu calea completă către directorul partajat în câmpul **Sursă**.

6. Fă clic pe **OK**.

7. În fila **Sursă**, debifează casetele de selectare de lângă numele surselor de actualizare pe care nu le-ai specificat drept director partajat.

8. Fă clic pe **OK**.

9. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Selectarea modului de executare a activității de actualizare

*Pentru a selecta modul de executare a activității de actualizare:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.

În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.

3. Fă clic pe butonul **Mod executare**.

Fila **Mod executare** se deschide în fereastra **Actualizare**.

4. În secțiunea **Mod executare**, selectează una dintre următoarele opțiuni pentru pornirea activității de actualizare:

- Dacă dorești ca aplicația Kaspersky Endpoint Security să execute activitatea de actualizare în funcție de disponibilitatea pachetului de actualizare în sursa de actualizare, selectează **Automat**. Frecvența cu care aplicația Kaspersky Endpoint Security verifică existența pachetelor de actualizare crește în timpul epidemiilor de viruși și scade în absența acestora.
- Dacă dorești să pornești manual o activitate de actualizare, selectează **Manual**.
- Dacă dorești să configurezi o planificare de pornire a activității de actualizare, selectează **După planificare**.

5. Efectuează una dintre următoarele acțiuni:

- Dacă ai selectat opțiunea **Automat** sau **Manual**, accesează pasul 6 al instrucțiunilor.

- Dacă ai selectat opțiunea **După planificare**, specifică setările pentru planificarea executării activității de actualizare. Pentru aceasta:
  - a. În lista verticală **Frecvență**, specifică momentul pornirii activității de actualizare. Selectează una dintre opțiunile următoare: **Minute**, **Ore**, **Zile**, **Săptămânal**, **La o oră specificată**, **Lunar** sau **După pornirea aplicației**.
  - b. În funcție de elementul selectat în lista verticală **Frecvență**, specifică valorile pentru setările care definesc ora pornirii activității de actualizare.
  - c. În câmpul **Amânare executare după pornirea aplicației timp de**, specifică intervalul de timp cu care să fie amânată pornirea activității de actualizare după pornirea aplicației Kaspersky Endpoint Security.

Dacă selectezi elementul **După pornirea aplicației** în lista verticală **Frecvență**, câmpul **Amânare executare după pornirea aplicației timp de** nu este disponibil.

- d. Dacă dorești ca aplicația Kaspersky Endpoint Security să execute cât mai curând posibil activitățile de actualizare omise, bifează caseta de selectare **Executare activități omise**.

Dacă selectezi **Ore**, **Minute** sau **După pornirea aplicației** în lista verticală **Frecvență**, caseta de selectare **Executare activități omise** este indisponibilă.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Pornirea unei activități de actualizare utilizând drepturile altui cont de utilizator

În mod implicit, activitatea de actualizare a aplicației Kaspersky Endpoint Security este pornită din partea utilizatorului al cărui cont l-ai utilizat pentru a face Log in la sistemul de operare. Totuși, aplicația Kaspersky Endpoint Security poate fi actualizată și dintr-o sursă de actualizare la care utilizatorul nu are acces din cauza lipsei drepturilor necesare (de exemplu, dintr-un director partajat care conține un pachet de actualizare) sau a nedeținerii drepturilor de utilizator autorizat pentru un server proxy. În setările aplicației Kaspersky Endpoint Security, poți specifica un utilizator care are astfel de drepturi și poți porni activitatea de actualizare a aplicației Kaspersky Endpoint Security din contul utilizatorului respectiv.

*Pentru a porni o activitate de actualizare din alt cont de utilizator:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Mod executare și sursă actualizare**, fă clic pe butonul **Mod executare**.  
Fila **Mod executare** se deschide în fereastra **Actualizare**.
4. În fila **Mod executare**, în secțiunea **Utilizator**, bifează caseta de selectare **Executare activitate ca**.
5. În câmpul **Nume**, introdu numele contului de utilizator ale cărui drepturi sunt necesare pentru accesarea sursei de actualizare.
6. În câmpul **Parolă**, introdu parola utilizatorului ale cărui drepturi sunt necesare pentru accesarea sursei de actualizare.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea actualizărilor pentru modulele aplicației

*Pentru a configura actualizările pentru modulele aplicației:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Suplimentar**, efectuează una dintre următoarele acțiuni:
  - Bifează caseta de selectare **Descărcare actualizări ale modulelor aplicației** dacă dorești ca aplicația să includă în pachetele de actualizare și actualizări de module ale aplicației.
  - În caz contrar, debifează caseta de selectare **Descărcare actualizări ale modulelor aplicației**.
4. Dacă ai bifat caseta de selectare **Descărcare actualizări ale modulelor aplicației** la pasul anterior, specifică condițiile în care aplicația va instala actualizările de module ale aplicației:
  - Selectează opțiunea **Instalare actualizări critice și aprobate** dacă dorești ca aplicația să instaleze în mod automat actualizări critice ale modulelor aplicației și alte actualizări, după

ce instalarea lor este aprobată, local prin interfața aplicației sau folosind Kaspersky Security Center.

- Selectează opțiunea **Instalare numai actualizări aprobate** dacă dorești ca aplicația să instaleze actualizări ale modulelor aplicației după ce instalarea lor este aprobată, local prin interfața aplicației sau folosind Kaspersky Security Center.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Pornirea și oprirea unei activități de actualizare

Indiferent de modul de executare a activității de actualizare pe care îl selectezi, poți porni sau opri oricând o activitate de actualizare a aplicației Kaspersky Endpoint Security.

Pentru a descărca un pachet de actualizare de pe serverele Kaspersky, ai nevoie de o conexiune la Internet.

*Pentru a porni sau a opri o activitate de actualizare:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Activități**.  
Se deschide secțiunea **Activități**.
4. Fă clic dreapta pentru a se afișa meniul contextual corespunzător liniei cu numele activității de actualizare.  
Se deschide un meniu cu acțiuni referitoare la activitatea de actualizare.
5. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să pornești activitatea de actualizare, selectează **Pornire actualizare** din meniu.  
Starea progresului activității de actualizare, care este afișată în partea dreaptă a butonului **Actualizare**, se schimbă în *În curs de executare*.
  - Dacă dorești să oprești activitatea de actualizare, selectează **Oprește actualizare** din meniu.  
Starea progresului activității de actualizare, care este afișată în partea dreaptă a butonului **Actualizare**, se schimbă în *oprit*.

## Derularea înapoi a celei mai recente actualizări

După prima actualizare a bazelor de date și modulelor aplicației, devine disponibilă funcția de derulare înapoi a bazelor de date și modulelor aplicației la versiunile lor anterioare.

De fiecare dată când utilizatorul pornește procesul de actualizare, aplicația Kaspersky Endpoint Security creează o copie de rezervă a bazelor de date și modulelor actuale ale aplicației. Acest lucru îți permite, atunci când este necesar, să derulezi înapoi bazele de date și modulele aplicației la versiunile lor anterioare. Derularea înapoi a celei mai recente actualizări este utilă, de exemplu, atunci când versiunea nouă a bazei de date conține o semnătură nevalidă care determină aplicația Kaspersky Endpoint Security să blocheze o aplicație sigură.

*Pentru a derula înapoi cea mai recentă actualizare:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Activități**.  
Se deschide secțiunea **Activități**.
4. Fă clic dreapta pentru a afișa meniul contextual al activității **Actualizare**.
5. Selectează **Restaurare actualizare**.

## Configurarea setărilor pentru serverul proxy

*Pentru a configura setările pentru serverul proxy:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Actualizare**.  
În partea dreaptă a ferestrei se afișează secțiunea Setări actualizare aplicație.
3. În secțiunea **Server proxy**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Setări server proxy**.
4. În fereastra **Setări server proxy**, bifează caseta de selectare **Utilizare server proxy**.
5. Specifică setările pentru serverul proxy.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Poți configura setările pentru serverul proxy inclusiv în fereastra principală a aplicației, în fila **Setări**, secțiunea **Setări avansate**.

## Scanarea computerului

O scanare de viruși este esențială pentru securitatea computerului. Scanările de viruși executate regulat contribuie la eliminarea posibilității de răspândire a programelor malware nedetectate de componentele protecției din cauza unei setări reduse a nivelului de securitate sau din alte motive.

În această secțiune sunt descrise elementele specifice și setările activităților de scanare, nivelurile de securitate, metodele și tehnologiile de scanare și instrucțiuni privind tratarea fișierelor pe care Kaspersky Endpoint Security nu le-a procesat în cursul unei scanări de viruși.

## Despre activitățile de scanare

Pentru a găsi viruși și alte tipuri de malware și pentru a verifica integritatea modulelor aplicației, Kaspersky Endpoint Security include următoarele activități:

- **Scanare completă.** O scanare completă a întregului computer. În mod implicit, Kaspersky Endpoint Security scanează următoarele obiecte:
  - Memorie kernel
  - Obiectele încărcate la pornirea sistemului de operare
  - Sectoarele de boot
  - Crearea unei copii de rezervă a sistemului de operare
  - Toate unitățile de disc și amovibile
- **Scanare zone critice.** În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor.
- **Scanare particularizată.** Kaspersky Endpoint Security scanează obiectele selectate de utilizator. Poți scana orice obiect din următoarea listă:
  - Memorie kernel
  - Obiectele încărcate la pornirea sistemului de operare
  - Crearea unei copii de rezervă a sistemului de operare
  - Cutia poștală Outlook



- Toate unitățile de disc, amovibile și din rețea
- Orice fișier selectat
- **Verificare integritate.** Kaspersky Endpoint Security verifică modulele aplicației pentru a vedea dacă sunt deteriorate sau modificate.

Activitățile Scanare completă și Scanare zone critice sunt într-o oarecare măsură diferite de altele. Pentru aceste activități, nu este recomandată editarea domeniului de scanare.

După pornirea operațiilor de scanare, progresul finalizării lor este afișat în câmpul din dreptul numelui activității de scanare care se execută, în secțiunea **Activități** din fila **Protecție și control** a ferestrei principale a Kaspersky Endpoint Security.

Informațiile despre rezultatele scanării și evenimentele care au apărut în timpul derulării activităților de scanare sunt înregistrate în raportul Kaspersky Endpoint Security.

## Pornirea și oprirea unei activități de scanare

Indiferent de modul de executare a activității de scanare pe care îl selectezi, poți porni sau opri oricând o activitate de scanare.

*Pentru a porni sau opri o activitate de scanare:*

1. Deschide [fereastra principală a aplicației](#).

2. Selectează fila **Protecție și control**.

3. Fă clic pe secțiunea **Activități**.

Se deschide secțiunea **Activități**.

4. Fă clic dreapta pentru a se afișa meniul contextual corespunzător liniei cu numele activității de scanare.

Se deschide un meniu care conține acțiunile pentru activitatea de scanare.

5. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să pornești activitatea de scanare, selectează **Pornire scanare** din meniu.  
Starea progresului activității afișată în dreapta butonului cu numele acestei activități de scanare se modifică în *Se execută*.
- Dacă dorești să oprești activitatea de scanare, selectează **Oprește scanare** din meniu.

Starea progresului activității afișată în dreapta butonului cu numele acestei activități de scanare se modifică în *Oprită*.

## Configurarea setărilor pentru o activitate de scanare

Pentru a configura setările pentru o activitate de scanare, poți efectua următoarele acțiuni:

- Schimbă nivelul de securitate.

Poți să selectezi unul dintre nivelurile de securitate presetate sau să configurezi manual setările pentru nivelul de securitate. Dacă modifizi setările pentru nivelul de securitate, poți reveni oricând la setările recomandate pentru nivelul de securitate.

- Schimbă acțiunea efectuată de Kaspersky Endpoint Security la detectarea unui fișier infectat.

- Editează domeniul de scanare.

Poți extinde sau restrânge domeniul de scanare adăugând sau eliminând obiecte de scanat sau schimbând tipurile de fișiere de scanat.

- Optimizează scanarea.

Poți optimiza scanarea fișierelor, reducând durata scanării și sporind viteza de funcționare a aplicației Kaspersky Endpoint Security. Acest lucru se obține prin scanarea numai a fișierelor noi și a celor care au fost modificate din momentul scanării ulterioare. Acest mod se aplică atât fișierelor simple, cât și celor compuse. De asemenea, poți seta o limită pentru scanarea unui fișier individual. După expirarea intervalului de timp specificat, Kaspersky Endpoint Security exclude fișierul din scanarea curentă (cu excepția arhivelor și a obiectelor care includ mai multe fișiere).

De asemenea, poți activa utilizarea tehnologiilor iChecker și iSwift. Aceste tehnologii optimizează viteza de scanare a fișierelor, excluzând fișierele care nu au fost modificate de la cea mai recentă scanare.

- Configurează scanarea fișierelor compuse.

- Configurează utilizarea metodelor de scanare.

Atunci când este activă, aplicația Kaspersky Endpoint Security utilizează analiza semnăturilor. La analiza semnăturii, Kaspersky Endpoint Security compară obiectul detectat cu înregistrările din bazele sale de date. În urma recomandărilor experților Kaspersky, analiza semnăturii este activată în permanență.

Pentru a spori eficiența protecției, poți utiliza analiza euristică. În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea obiectelor în sistemul de operare. Analiza euristică poate detecta obiecte rău intenționate pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

- Selectează modul de executare a activității de scanare.

Dacă nu se poate executa activitatea de scanare dintr-un anumit motiv (de exemplu, computerul este oprit la momentul respectiv), poți configura activitatea omisă pentru executare automată atunci când este posibil.

Poți amâna activitatea de scanare după pornirea aplicației dacă ai selectat modul de executare a activității de actualizare **După planificare** și ora de pornire a aplicației Kaspersky Endpoint Security corespunde planificării executării activității de scanare. Activitatea de scanare se poate executa numai după scurgerea intervalului de timp specificat de la pornirea aplicației Kaspersky Endpoint Security.

- Configurează activitatea de scanare pentru executare din alt cont de utilizator.
- Specifică setările pentru scanarea mediilor amovibile la conectarea acestora.

## Schimbarea nivelului de securitate

Pentru a efectua activități de scanare, Kaspersky Endpoint Security utilizează diverse combinații de setări. Aceste combinații de setări salvate în aplicație sunt denumite *niveluri de securitate*. Sunt preinstalate trei niveluri de securitate presetate: **Ridicat**, **Recomandat** și **Redus**. Setările pentru nivelul de securitate **Recomandat** sunt considerate optime. Ele sunt recomandate de experții Kaspersky.

*Pentru a modifica un nivel de securitate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).  
În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.
3. În secțiunea **Nivel de securitate**, efectuează una dintre următoarele acțiuni:
  - Dacă dorești să aplici unul dintre nivelurile de securitate presetate (**Ridicat**, **Recomandat** sau **Redus**), selectează-l folosind cursorul.
  - Dacă dorești să configurezi un nivel de securitate particularizat, fă clic pe butonul **Setări** și, în fereastra care se deschide, specifică setările cu numele activității de scanare.  
După ce configurezi un nivel particularizat de securitate, numele nivelului de securitate din secțiunea **Nivel de securitate** devine **Particularizat**.
  - Dacă dorești ca nivelul de securitate să devină cel **Recomandat**, fă clic pe butonul **Implicit**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Schimbarea acțiunii de efectuat asupra fișierelor infectate

*Pentru a schimba acțiunea de efectuat asupra fișierelor infectate:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. În secțiunea **Acțiune la detectarea amenințării**, selectează opțiunea necesară:

- **Selectare automată acțiune.**
- **Efectuare acțiune.**

4. Dacă ai selectat opțiunea **Efectuare acțiune** în pasul anterior, bifează următoarele casete de selectare:

- Bifează caseta de selectare **Dezinfectare** dacă dorești ca aplicația Kaspersky Endpoint Security să dezinfecteze obiectele în care au fost detectate amenințări.

Chiar dacă această opțiune este selectată, Kaspersky Endpoint Security aplică acțiunea **Eliminare** fișierelor care fac parte din aplicația Windows Store.

- Bifează caseta de selectare **Ștergere** dacă dorești ca aplicația Kaspersky Endpoint Security să șteargă obiectele în care sunt detectate amenințări.
- Bifează ambele casete de selectare **Dezinfectare** și **Ștergere** dacă dorești ca aplicația Kaspersky Endpoint Security să încerce să dezinfecteze obiectele în care sunt detectate amenințări și să șteargă obiectele care nu pot fi dezinfectate.
- Debifează ambele casete de selectare **Dezinfectare** și **Ștergere** dacă dorești ca aplicația Kaspersky Endpoint Security să nu întreprindă nicio acțiune asupra obiectelor în care sunt detectate amenințări, ci doar să-l notifice pe utilizator asupra rezultatelor scanării acestor obiecte.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Generarea unei liste de obiecte de scanat

Pentru a genera o listă de obiecte de scanat, poți utiliza una dintre următoarele două metode:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

Această metodă este disponibilă numai pentru activitățile **Scanare completă** și **Scanare zone critice**. Lista de obiecte de scanat pentru activitatea **Scanare particularizată** poate fi creată numai în fila **Protecție și control**.

*Pentru a crea o listă de obiecte de scanat în fila Protecție și control, din fereastra principală a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Activități**.  
Se deschide secțiunea **Activități**.
4. Fă clic dreapta pentru a se deschide meniul contextual al liniei care conține numele activității și selectează **Domeniu de scanare**.  
Se deschide fereastra **Domeniu de scanare**.
5. Dacă dorești să adaugi un obiect nou la domeniul de scanare:
  - a. Fă clic pe butonul **Adăugare**.  
Se deschide fereastra **Selectare domeniu de scanare**.
  - b. Selectează obiectul și apasă pe **Adăugare**.  
Toate obiectele selectate în fereastra **Selectare domeniu de scanare** sunt afișate în lista **Domeniu de scanare**.
  - c. Fă clic pe **OK**.
6. Dacă dorești să modifice calea către un obiect din domeniul de scanare:
  - a. Selectează obiectul în domeniul de scanare.
  - b. Fă clic pe butonul **Editare**.  
Se deschide fereastra **Selectare domeniu de scanare**.
  - c. Introdu o cale nouă către obiect în domeniul de scanare.

d. Fă clic pe **OK**.

7. Dacă dorești să ștergi un obiect din domeniul de scanare:

a. Selectează obiectul pe care vrei să-l ștergi din domeniul de scanare.

Pentru a selecta obiecte multiple, selectează-le în timp ce ții apăsată tasta **CTRL**.

b. Fă clic pe butonul **Eliminare**.

Se deschide o fereastră pentru confirmarea ștergerii.

c. Apasă pe **Da** în fereastra de confirmare a ștergerii.

Nu poți șterge sau edita obiecte care sunt incluse în domeniul de scanare implicit.

8. Pentru a exclude un obiect din domeniul de scanare, debifează caseta de selectare de lângă obiect în fereastra **Domeniu de scanare**.

Obiectul rămâne în lista de obiecte din domeniul de scanare, însă nu va fi scanat la executarea activității de scanare.

9. Fă clic pe **OK**.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

*Pentru a crea o listă de obiecte de scanat din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea cu numele activității de scanare necesare: **Scanare completă** sau **Scanare zone critice**.

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. Fă clic pe butonul **Domeniu de scanare**.

Se deschide fereastra **Domeniu de scanare**.

4. Creează o listă de obiecte de scanat conform pașilor 5 – 10 ai instrucțiunilor anterioare.

## Selectarea unui tip de fișiere de scanat

Poți folosi următoarele două metode pentru a selecta tipul de fișiere de scanat:

- În fila **Protecție și control** din [fereastra principală a aplicației](#)
- Din [fereastra cu setările aplicației](#)

Această metodă este disponibilă numai pentru activitățile **Scanare completă** și **Scanare zone critice**. Tipul de fișiere de scanat pentru activitatea **Scanare particularizată** poate fi selectat numai în fila **Protecție și control**.

*Pentru a selecta tipul de fișiere de scanat în fila Protecție și control a ferestrei principale a aplicației:*

1. Deschide fereastra principală a aplicației.
2. Selectează fila **Protecție și control**.
3. Fă clic pe secțiunea **Activități**.  
Se deschide secțiunea **Activități**.
4. Fă clic dreapta pentru a deschide meniul contextual al liniei care conține numele activității și selectează **Setări**.  
Se deschide o fereastră cu numele activității de scanare selectate.
5. În fereastra cu numele activității de scanare selectate, selectează fila **Domeniu**.
6. În secțiunea **Tipuri de fișiere**, specifică tipurile de fișiere care dorești să fie scanate la executarea activității de scanare selectate:
  - Dacă dorești să scanezi toate fișierele, selectează **Toate fișierele**.
  - Dacă dorești să scanezi fișierele ale căror formate sunt cele mai vulnerabile la infectare, selectează **Fișiere scanate după format**.
  - Dacă dorești să scanezi fișierele ale căror extensii sunt de obicei cele mai vulnerabile la infectare, selectează **Fișiere scanate după extensie**.

Când selectezi tipurile de fișiere de scanat, ia în calcul următoarele:

- Există unele formate de fișiere (precum TXT) pentru care există o probabilitate redusă de pătrundere a unui cod rău intenționat și de activare ulterioară a acestuia. În același timp, există formate de fișiere care conțin sau pot conține cod executabil (precum .exe, .dll și .doc). Riscul de pătrundere și de activare a codului rău intenționat în astfel de fișiere este ridicat.
- Un intrus poate trimite pe computerul tău un virus sau alt program rău intenționat într-un fișier executabil care a fost redenumit cu extensia .txt. Dacă selectezi scanarea fișierelor după extensie, aplicația omite acest fișiere în cursul scanării. Dacă este selectată scanarea fișierelor după format, componenta Antivirus pentru fișiere analizează antetul fișierului indiferent de extensie. Dacă această analiză arată că fișierul are formatul EXE, aplicația îl scanează.

7. În fereastra care conține numele unei activități de scanare, fă clic pe butonul **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

*Pentru a selecta tipul de fișiere de scanat din fereastra cu setările aplicației:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea cu numele activității de scanare necesare: **Scanare completă** sau **Scanare zone critice**.

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide o fereastră cu numele activității de scanare selectate.

4. În fereastra cu numele activității de scanare selectate, selectează fila **Domeniu**.

5. Finalizează pașii 5–7 ai instrucțiunilor anterioare.

## Optimizarea scanării de fișiere

*Pentru a optimiza scanarea de fișiere:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide o fereastră cu numele activității de scanare selectate.

4. În fereastra care se deschide, selectează fila **Domeniu**.

5. În secțiunea **Optimizare scanare**, efectuează următoarele acțiuni:

- Bifează caseta de selectare **Scanare numai fișiere noi și modificate**.
- Bifează caseta de selectare **Se ignoră fișierele scanate mai mult de** și specifică durata scanării pentru un singur fișier (în secunde).

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.



## Scanarea fișierelor compuse

O tehnică obișnuită de ascundere a virușilor și a altor programe malware o reprezintă introducerea acestora în fișiere compuse, precum arhive sau baze de date. Pentru a detecta virușii și celelalte programe malware ascunse în acest mod, fișierul compus trebuie dezarhivat, fapt care poate încetini scanarea. Poți limita tipurile de fișiere compuse de scanat, accelerând astfel scanarea.

*Pentru a configura scanarea fișierelor compuse:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide o fereastră cu numele activității de scanare selectate.

4. În fereastra care se deschide, selectează fila **Domeniu**.

5. În secțiunea **Scanare fișiere compuse**, specifică fișierele compuse pe care dorești să le scanezi: arhive, pachete de instalare, fișiere în formate Office, fișiere în format corespondență și arhive protejate prin parolă.

6. Dacă este debifată caseta de selectare **Scanare numai fișiere noi și modificate** în secțiunea **Optimizare scanare**, fă clic pe linkul **toate/noi** de lângă numele unui fișier compus dacă dorești să specifice în cazul fiecărui tip de fișier compus dacă se scanează toate fișierele de acest tip sau numai cele noi.

Acest link își schimbă valoarea atunci când faci clic pe el.

În cazul în care caseta de selectare **Scanare numai fișiere noi și modificate** este bifată, se vor scana numai fișierele noi.

7. Fă clic pe butonul **Suplimentar**.

Se deschide fereastra **Fișiere compuse**.

8. În secțiunea **Limită dimensiune**, efectuează una dintre următoarele acțiuni:

- Dacă nu dorești să dezarhivezi fișierele compuse de dimensiuni mari, bifează caseta de selectare **Nu dezarhiva fișiere compuse mari** și specifică valoarea necesară în câmpul **Dimensiune maximă fișier**.

- Dacă dorești să dezarhivezi fișiere compuse de dimensiuni mari, indiferent de dimensiunea lor, debifează caseta de selectare **Nu dezarhiva fișiere compuse mari**.

Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișiere compuse mari**.

9. Fă clic pe **OK**.

10. În fereastra care conține numele activității de scanare, fă clic pe butonul **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Utilizarea metodelor de scanare

*Pentru a utiliza metode de scanare:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).

În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.

3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.

Se deschide o fereastră cu numele activității de scanare selectate.

4. În fereastra care se deschide, selectează fila **Suplimentar**.

5. Dacă dorești ca aplicația să utilizeze analiza euristică la executarea activității de scanare, în secțiunea **Metode de scanare**, bifează caseta de selectare **Analiză euristică**. Apoi utilizează cursorul pentru a seta nivelul analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Utilizarea tehnologiilor de scanare

*Pentru a utiliza tehnologii de scanare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității de scanare necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).  
În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.
3. În secțiunea **Nivel de securitate**, fă clic pe butonul **Setări**.  
Se deschide o fereastră cu numele activității de scanare selectate.
4. În fereastra care se deschide, selectează fila **Suplimentar**.
5. În secțiunea **Tehnologii de scanare**, bifează casetele de selectare de lângă numele tehnologiilor care doriți să fie utilizate la scanare.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Selectarea modului de executare pentru activitatea de scanare

*Pentru a selecta modul de executare a activității de scanare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).  
În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.
3. Fă clic pe butonul **Mod executare**.  
O fereastră cu proprietățile activității selectate se deschide în fila **Mod executare**.
4. În secțiunea **Mod executare**, selectează modul de executare a activității: **Manual** sau **După planificare**.
5. Dacă ai selectat opțiunea **După planificare**, specifică setările pentru planificare. Pentru aceasta:
  - a. În lista verticală **Frecvență**, selectează frecvența activității (**Minute**, **Ore**, **Zile**, **Săptămânal**, **La o oră specificată**, **Lunar** sau **După pornirea aplicației**, **După fiecare actualizare**).
  - b. În funcție de frecvența selectată, configurează setările avansate pentru a specifica planificare de executare a activității.

- c. Dacă dorești ca aplicația Kaspersky Endpoint Security să execute cât mai curând posibil activitățile de scanare omise, bifează caseta de selectare **Executare activități omise**.

Dacă selectezi elementul **Minute, Ore, După pornirea aplicației** sau **După fiecare actualizare** în lista verticală **Frecvență**, caseta de selectare **Executare activități omise** este indisponibilă.

- a. Dacă dorești ca aplicația Kaspersky Endpoint Security să suspende o activitate atunci când resursele computerului sunt limitate, bifează caseta de selectare **Execută doar atunci când computerul este inactiv**.

Această opțiune de planificare ajută la conservarea resurselor computerului.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Pornirea unei activități de scanare din contul altui utilizator

În mod implicit, o activitate de scanare se execută cu permisiunile contului în care utilizatorul s-a conectat la sistemul de operare. Cu toate acestea, este posibil să fie necesar să execuți o activitate de scanare din alt cont de utilizator. Poți să specificezi un utilizator care are drepturile corespunzătoare în setările pentru activitatea de scanare și să execuți activitatea de scanare din contul acestui utilizator.

*Pentru a configura pornirea unei activități de scanare din contul altui utilizator:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează subsecțiunea care conține numele activității necesare (**Scanare completă**, **Scanare zone critice** sau **Scanare particularizată**).  
În partea dreaptă a ferestrei se afișează setările activității de scanare selectate.
3. Fă clic pe butonul **Mod executare**.  
Această acțiune deschide o fereastră cu proprietățile activității selectate în fila **Mod executare**.
4. În fila **Mod executare**, în secțiunea **Utilizator**, bifează caseta de selectare **Executare activitate ca**.
5. În câmpul **Nume**, introdu numele contului de utilizator ale cărui drepturi sunt necesare pentru lansarea activității de scanare.

6. În câmpul **Parolă**, introdu parola utilizatorului ale cărei drepturi sunt necesare pentru lansarea activității de scanare.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Scanarea unităților amovibile atunci când sunt conectate la computer

Unele programe rău intenționate exploatează vulnerabilitățile sistemului de operare pentru a se înmulți în rețelele locale și pe unitățile amovibile. Kaspersky Endpoint Security permite scanarea unităților amovibile conectate al computer pentru detectarea virusilor și a altor programe malware.

*Pentru a configura scanarea unităților amovibile atunci când acestea sunt conectate:*


1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Activități planificate**.  
Setările activității sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Scanare unități amovibile la conectare**, selectează acțiunea necesară în lista verticală **Acțiune la conectare unitate amovibilă**:

- **Nu scana**

- **Scanare detaliată**

În acest mod, Kaspersky Endpoint Security scanează toate fișierele amplasate pe unitatea amovibilă, inclusiv fișierele din obiectele compuse.

- **Scanare rapidă**

În acest mod, Kaspersky Endpoint Security scanează numai [fișiere potențial infectabile](#)  și nu despachetează obiecte compuse.

4. Dacă dorești ca aplicația Kaspersky Endpoint Security să scaneze doar unitățile amovibile a căror capacitate nu depășește valoarea specificată, bifează caseta de selectare **Dimensiune maximă unitate amovibilă** și specifică în câmpul alăturat o valoare în megaocteți.
5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Tratarea fișierelor neprocesate

Această secțiune conține instrucțiuni despre tratarea fișierelor infectate și probabil infectate pe care Kaspersky Endpoint Security nu le-a procesat în cursul scanării computerului după viruși și alte amenințări.

## Despre fișierele neprocesate

Kaspersky Endpoint Security înregistrează în jurnal informațiile despre fișierele neprocesate dintr-un anumit motiv. Aceste informații sunt înregistrate sub forma unor evenimente în lista de fișiere neprocesate.

Un fișier infectat este considerat *procesat* dacă aplicația Kaspersky Endpoint Security execută una dintre următoarele acțiuni asupra acestui fișier, în conformitate setările de aplicație specificate în cursul scanării computerului după viruși și alte amenințări:

- Dezinfectare.
- Eliminare.
- Ștergere dacă dezinfectarea nu reușește.

Un fișier infectat este considerat *neprocesat* dacă aplicația Kaspersky Endpoint Security, indiferent de motiv, nu reușește să execute o acțiune asupra acestui fișier, potrivit setărilor de aplicație specificate în cursul scanării computerului după viruși și alte amenințări.

Această situație este posibilă în următoarele cazuri:

- Fișierul scanat este indisponibil (de exemplu, este localizat pe o unitate de rețea sau pe o unitate amovibilă, fără privilegii de scriere).
- Acțiunea selectată în secțiunea **Acțiune la detectarea amenințării** pentru activitățile de scanare este **Informare**, iar utilizatorul selectează acțiunea **Omitere** atunci când este afișată o notificare despre fișierul infectat.

Poți porni manual o activitate de scanare particularizată pentru fișiere neprocesate după actualizarea bazei de date și a modulelor aplicației. Starea fișierului se poate modifica după scanare. Poți efectua acțiunile necesare asupra fișierelor, în funcție de starea lor.

De exemplu, poți efectua următoarele acțiuni:

- [Ștergerea fișierelor cu stare \*Infectat\*](#).
- Restaurarea fișierelor infectate care conțin informații importante și restaurarea fișierelor marcate ca *Dezinfectate* sau *Neinfectate*.
- Plasarea în Carantină a fișierelor cu starea *Probabil infectat*.

## Gestionarea listei de fișiere neprocesate

Lista de fișiere neprocesate apare sub forma unui tabel.

Poți efectua următoarele operațiuni cu fișiere neprocesate:

- Vizualizarea listei de fișiere neprocesate.
- Scanarea fișierelor neprocesate utilizând versiunea curentă a bazelor de date și modulelor Kaspersky Endpoint Security.
- Restaurarea fișierelor din lista de fișiere neprocesate în directoarele inițiale sau într-un alt director, la latitudinea ta (atunci când nu se poate scrie în directorul inițial).
- Eliminarea fișierelor din lista de fișiere neprocesate.
- Deschiderea directorului în care a fost amplasat inițial fișierul neprocesat.

Poți efectua și următoarele acțiuni în timpul gestionării datelor din tabel:

- Filtrează evenimentele de fișiere neprocesate după valorile coloanei sau utilizând condiții de filtrare particularizate.
- Utilizarea funcției de căutare a evenimentelor de fișiere neprocesate.
- Sortarea evenimentelor de fișiere neprocesate.
- Schimbarea ordinii și setarea coloanelor de afișat în lista de evenimente de fișiere neprocesate.
- Gruparea evenimentelor de fișiere neprocesate.

Dacă este necesar, poți copia în clipboard evenimente selectate de fișiere neprocesate.

## Pornirea unei activități de scanare particularizată pentru fișiere neprocesate

Poți porni manual o activitate de scanare particularizată pentru fișiere neprocesate. Poți porni activitatea dacă, de exemplu, ultima scanare a fost întreruptă dintr-un motiv oarecare sau dacă dorești să scanezi din nou fișiere neprocesate după ultima actualizare a bazelor de date și a modulelor aplicației.

*Pentru a porni o scanare particularizată a fișierelor neprocesate:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Fișiere neprocesate**.
4. În tabelul din fila **Fișiere neprocesate**, selectează unul sau mai multe evenimente asociate cu fișierele pe care dorești să le scanezi.  
Pentru a selecta evenimente multiple, selectează-le în timp ce ții apăsată tasta **CTRL**.
5. Pornește activitatea de scanare particularizată într-unul din modurile următoare:
  - Fă clic pe butonul **Repetare scanare**.
  - Fă clic dreapta pentru a afișa meniul contextual și selectează **Repetare scanare**.

## Ștergerea fișierelor din lista de fișiere neprocesate

*Pentru a șterge fișiere din lista de fișiere neprocesate:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Fișiere neprocesate**.
4. În tabelul din fila **Fișiere neprocesate**, selectează unul sau mai multe evenimente asociate cu fișierele pe care dorești să le ștergi.  
Pentru a selecta evenimente multiple, selectează-le în timp ce ții apăsată tasta **CTRL**.
5. Șterge fișierele într-unul din modurile următoare:
  - Fă clic pe butonul **Eliminare**.
  - Fă clic dreapta pentru a deschide meniul contextual și selectează **Ștergere**.

## Scanarea de vulnerabilități

Această secțiune conține informații despre aspectele specifice și setările pentru activitatea Scanare de vulnerabilități, precum și instrucțiuni privind gestionarea listei de vulnerabilități detectate de Kaspersky Endpoint Security la executarea activității Scanare de vulnerabilități.

## Vizualizarea informațiilor despre vulnerabilitățile aplicațiilor în curs de executare



Informațiile despre vulnerabilitățile din aplicațiile în execuție sunt disponibile dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Microsoft Windows pentru stații de lucru. Aceste informații nu sunt disponibile dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută [Microsoft Windows pentru servere de fișiere](#).

*Pentru a vizualiza informațiile despre vulnerabilitățile aplicațiilor în execuție:*

1. Deschide [fereastra principală a aplicației](#).
2. Selectează fila **Protecție și control**.
3. Deschide secțiunea **Control endpoint**.
4. Fă clic pe butonul **Monitorizare activitate aplicație**.

Se deschide fereastra **Control drepturi aplicații** în fila **Monitorizare activitate aplicație**. Tabelul **Monitor activitate aplicație** prezintă informații rezumat despre activitatea aplicațiilor care se execută pe sistemul de operare. În coloana **Gravitatea vulnerabilității** este prezentată gravitatea vulnerabilității pentru aplicațiile în execuție, așa cum este ea determinată de către componenta Monitor de vulnerabilități.

## Despre activitatea Scanare de vulnerabilități

Vulnerabilitățile din sistemul de operare pot fi cauzate, de exemplu, de erori de programare sau de proiectare, de parole slabe sau de activități ale programelor malware. Atunci când scanează pentru detectarea vulnerabilităților, aplicația analizează sistemul de operare și caută anomalii și setări alterate ale aplicațiilor de la Microsoft și de la alți producători de software.

O scanare pentru detectarea vulnerabilităților efectuează o diagnosticare a securității sistemului de operare și detectează caracteristici software care pot fi utilizate de intruși pentru a răspândi obiecte rău intenționate și a obține acces la informații personale.

După [pornirea activității Scanare de vulnerabilități](#), progresul său este afișat în câmpul din dreptul numelui activității **Scanare de vulnerabilități**, în secțiunea **Activități** din fila **Protecție și control** a ferestrei principale a Kaspersky Endpoint Security.

Rezultatele activității Scanare de vulnerabilități se înregistrează în [rapoarte](#).

## Pornirea și oprirea activității Scanare de vulnerabilități

Indiferent de modul de executare selectat pentru activitatea Scanare de vulnerabilități, poți porni sau opri activitatea în orice moment.

*Pentru a porni și a opri activitatea Scanare de vulnerabilități:*

1. Deschide [fereastra principală a aplicației](#).

2. Selectează fila **Protecție și control**.

3. Fă clic pe secțiunea **Activități**.

Se deschide secțiunea **Activități**.

4. Fă clic dreapta pentru a afișa meniul contextual corespunzător liniei cu numele activității Scanare de vulnerabilități.

Se deschide un meniu cu operațiunile pentru activitatea Scanare de vulnerabilități.

5. Efectuează una dintre următoarele acțiuni:

- Pentru a porni activitate Scanare de vulnerabilități, selectează **Pornire scanare** din meniu.  
Starea progresului activității afișată în dreapta butonului cu numele activității Scanare de vulnerabilități se modifică în *Se execută*.
- Pentru a opri activitate Scanare de vulnerabilități, selectează **Oprește scanare** din meniu.  
Starea progresului activității afișată în dreapta butonului cu numele activității Scanare de vulnerabilități se modifică în *Oprită*.

## Configurarea setărilor Scanare de vulnerabilități

Pentru a configura setările pentru Scanare de vulnerabilități, poți efectua următoarele acțiuni:

- Creează domeniul de scanare de vulnerabilități.  
Poți extinde sau reduce domeniul de scanare adăugând sau eliminând aplicații care să fie scanate de vulnerabilități.
- Selectarea modului de executare pentru activitatea Scanare de vulnerabilități.  
Dacă nu se poate executa activitatea dintr-un anumit motiv (de exemplu, computerul este oprit la momentul respectiv), poți configura activitatea omisă să se execute automat atunci când este posibil.
- Configurează activitatea să se execute sub un alt cont de utilizator.

În mod implicit, o activitate de scanare se execută cu permisiunile contului în care utilizatorul s-a conectat la sistemul de operare. Cu toate acestea, este posibil să fie necesar să execuți o activitate de scanare din alt cont de utilizator. Poți să specifici un utilizator care are drepturile corespunzătoare în setările activității și să execuți activitatea sub contul acestui utilizator.

## Crearea unui domeniu de scanare de vulnerabilități

Domeniul unei scanări de vulnerabilități acoperă un vânzător de software sau o cale către directorul în care a fost instalat programul software (de exemplu, toate aplicațiile Microsoft instalate în directorul Fișiere program).

*Pentru a crea un domeniu de scanare de vulnerabilități:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Scanare de vulnerabilități**.

În partea dreaptă a ferestrei sunt afișate setările pentru activitatea Scanare de vulnerabilități.

3. În secțiunea **Domeniu de scanare**:

a. Pentru a utiliza Kaspersky Endpoint Security în scopul vizualizării vulnerabilităților din aplicațiile Microsoft instalate pe computer, bifați caseta de selectare **Microsoft**.

b. Pentru a utiliza Kaspersky Endpoint Security în scopul vizualizării vulnerabilităților din toate aplicațiile instalate pe un computer care nu este Microsoft, bifați caseta de selectare **Alți furnizori**.

c. În fereastra **Zonă suplimentară de scanare pentru vulnerabilități**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Domeniu de scanare pentru vulnerabilități**.

d. Creează domeniul de scanare pentru vulnerabilități. În acest scop, utilizează butoanele **Adăugare** și **Eliminare**.

e. În fereastra **Domeniu de scanare pentru vulnerabilități**, fă clic pe **OK**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Selectarea modului de executare pentru activitatea Scanare de vulnerabilități

*Pentru a selecta modul de executare a activității Scanare de vulnerabilități:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Scanare de vulnerabilități**.

În partea dreaptă a ferestrei sunt afișate setările pentru activitatea Scanare de vulnerabilități.

3. Fă clic pe butonul **Mod executare**.

Această acțiune deschide fila **Mod executare** din fereastra **Scanare de vulnerabilități**.

4. În secțiunea **Mod executare**, selectează una dintre următoarele opțiuni pentru modul de executare pentru activitatea Scanare de vulnerabilități:

- Dacă dorești să pornești manual activitatea Scanare de vulnerabilități, selectează **Manual**.
- Dacă dorești să configurezi o planificare de pornire a activității Scanare de vulnerabilități, selectează **După planificare**.

5. Efectuează una dintre următoarele acțiuni:

- Dacă ai selectat opțiunea **Manual**, accesează pasul 6 al acestor instrucțiuni.
- Dacă ai selectat opțiunea **După planificare**, specifică setările de pornire pentru activitatea Scanare de vulnerabilități. Pentru aceasta:
  - a. În lista verticală **Frecvență**, specifică momentul pornirii activității Scanare de vulnerabilități. Selectează una dintre opțiunile următoare: **Zile**, **Săptămânal**, **La o oră specificată**, **Lunar**, **După pornirea aplicației** sau **După fiecare actualizare**.
  - b. În funcție de elementul selectat în lista verticală **Frecvență**, specifică valorile pentru setările care definesc ora pornirii activității Scanare de vulnerabilități.
  - c. Dacă dorești ca aplicația Kaspersky Endpoint Security să pornești cât mai curând posibil activitățile Scanare de vulnerabilități omise, bifează caseta de selectare **Executare activități omise**.

Dacă selectezi **După pornirea aplicației** sau **După fiecare actualizare** în lista verticală **Frecvență**, caseta de selectare **Executare activități omise** este indisponibilă.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

**Pornirea activității Scanare de vulnerabilități utilizând drepturile unui alt cont de utilizator**

În mod implicit, activitatea Scanare de vulnerabilități este pornită din contul cu care utilizatorul s-a conectat la sistemul de operare. Cu toate acestea, este posibil să fie nevoie să pornești activitatea Scanare de vulnerabilități sub alt cont de utilizator. Poți să specificezi un utilizator care are aceste drepturi în setările pentru activitatea Scanare de vulnerabilități și să pornești activitatea Scanare de vulnerabilități din contul acestui utilizator.

*Pentru a configura lansarea activității Scanare de vulnerabilități din alt cont de utilizator:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Scanare de vulnerabilități**.  
În partea dreaptă a ferestrei sunt afișate setările pentru activitatea Scanare de vulnerabilități.
3. Fă clic pe butonul **Mod executare**.  
Această acțiune deschide fila **Mod executare** din fereastra **Scanare de vulnerabilități**.
4. În fila **Mod executare**, în secțiunea **Utilizator**, bifează caseta de selectare **Executare activitate ca**.
5. În câmpul **Nume**, introdu numele de cont al utilizatorului ale cărui drepturi sunt necesare pentru pornirea activității Scanare de vulnerabilități.
6. În câmpul **Parolă**, introdu parola utilizatorului ale cărui drepturi sunt necesare pentru pornirea activității Scanare de vulnerabilități.
7. Fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Gestionarea listei de vulnerabilități

Atunci când gestionezi lista de vulnerabilități, poți efectua următoarele acțiuni:

- Vizualizarea listei de vulnerabilități.
- Repornirea activității Scanare de vulnerabilități după actualizarea bazelor de date și a modulelor aplicației.
- Vizualizarea unor informații detaliate despre vulnerabilitate și a recomandărilor privind remedierea acesteia, într-o secțiune separată.
- Ascunderea înregistrărilor selectate în lista de vulnerabilități.
- Filtarea listei de vulnerabilități după nivelul de importanță.

- Filtrarea listei de vulnerabilități după valorile de stare *Remediat* și *Ascuns*.

Poți efectua și următoarele acțiuni în timpul gestionării datelor din tabel:

- Filtrarea listei de vulnerabilități după valorile coloanei sau utilizând condiții de filtrare particularizate.
- Utilizarea funcției de căutare a vulnerabilităților.
- Sortarea înregistrărilor din lista de vulnerabilități.
- Modificare ordine și aranjare coloane prezentate în lista de vulnerabilități.
- Gruparea înregistrărilor din lista de vulnerabilități.



## Despre lista de vulnerabilități


Kaspersky Endpoint Security înregistrează în jurnal rezultatele [activității Scanare de vulnerabilități](#) în lista de vulnerabilități.

După ce examinezi vulnerabilitățile selectate și efectuezi acțiunile care sunt recomandate pentru remedierea lor, Kaspersky Endpoint Security modifică starea vulnerabilităților la *Remediat*.

Dacă nu dorești să se afișeze înregistrările despre anumite vulnerabilități în lista de vulnerabilități, poți alege să ascundă aceste înregistrări. Kaspersky Endpoint Security atribuie acestor vulnerabilități starea *Ascuns*.

Lista de vulnerabilități apare sub forma unui tabel. Fiecare rând din tabel conține următoarele informații:

- O pictogramă care semnifică nivelul de gravitate a vulnerabilității. Sunt disponibile următoarele nivele de gravitate pentru vulnerabilități:
  - Pictogramă  **Critice**. Acest nivel de gravitate se aplică vulnerabilităților periculoase, care trebuie să fie remediate fără întârziere. Intrușii exploatează activ vulnerabilitățile de acest nivel pentru a infecta sistemul de operare al computerului sau pentru a accesa datele personale ale utilizatorului. Kaspersky recomandă luarea tuturor măsurilor necesare pentru remedierea vulnerabilităților cu nivelul de gravitate „Critic”.
  - Pictogramă  **Importante**. Acest nivel de gravitate se aplică vulnerabilităților importante care trebuie să fie remediate rapid. Intrușii pot exploata activ vulnerabilitățile de acest nivel. Intrușii nu exploatează în prezent în mod activ vulnerabilitățile de la nivelul de gravitate „Important”. Kaspersky recomandă luarea tuturor măsurilor necesare pentru remedierea vulnerabilităților cu nivelul de gravitate „Important”.

- Pictogramă . **Avertizare.** Acest nivel de gravitate se aplică pentru vulnerabilitățile a căror remediere poate fi amânată. Aceste vulnerabilități pot periclita însă pe viitor securitatea computerului.
- ID vulnerabilitate.
- Numele aplicației în care este detectată vulnerabilitatea.
- Scurtă descriere a vulnerabilității.
- Informații despre distribuitorul programului software, așa cum se indică în semnătura digitală.
- Rezultatul acțiunilor efectuate pentru remedierea vulnerabilității.

## Repornirea unei activități Scanare de vulnerabilități

Pentru a actualiza informațiile despre vulnerabilitățile detectate anterior, poți reporni activitatea Scanare de vulnerabilități. Este posibil să fie nevoie să repornești activitatea de scanare dacă scanarea de vulnerabilități a fost întreruptă din indiferent ce motiv sau dacă dorești să scanezi computerul de vulnerabilități după cea mai recentă [actualizare a bazelor de date și a modulelor aplicației](#).

*Pentru a reporni o activitate Scanare de vulnerabilități:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Vulnerabilități**.

Fila **Vulnerabilități** conține o listă de vulnerabilități pe care Kaspersky Endpoint Security le-a detectat în cursul activității Scanare de vulnerabilități.
4. În colțul din dreapta jos al ferestrei **Stocări**, fă clic pe butonul **Repetare scanare**.

Kaspersky Endpoint Security actualizează informațiile detaliate despre vulnerabilități în lista de vulnerabilități.

Starea unei vulnerabilități care a fost remediată prin instalarea unei corecții propuse nu se modifică după o altă scanare de vulnerabilități.

## Remedierea unei vulnerabilități

Poți remedia o vulnerabilitate instalând o actualizare a sistemului de operare, modificând configurația aplicației sau instalând o corecție de aplicație.

Vulnerabilitățile detectate nu se pot aplica aplicațiilor instalate, ci copiilor acestora. O corecție poate remedia o vulnerabilitate numai dacă aplicația este instalată.

*Pentru a remedia o vulnerabilitate:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Vulnerabilități**.


Fila **Vulnerabilități** conține o listă de vulnerabilități pe care Kaspersky Endpoint Security le-a detectat în cursul activității Scanare de vulnerabilități.

4. În lista de vulnerabilități, selectează înregistrarea care corespunde vulnerabilității respective.

În partea de jos a listei de vulnerabilități se deschide o secțiune cu informații despre această vulnerabilitate și recomandări pentru remedierea ei.

Informațiile următoare sunt disponibile pentru fiecare vulnerabilitate selectată:

- Numele aplicației în care este detectată vulnerabilitatea.
- Versiunea aplicației în care este detectată vulnerabilitatea.
- Nivelul de gravitate pentru o vulnerabilitate.
- ID vulnerabilitate.
- Data și ora ultimei detectări de vulnerabilitate.
- Recomandări pentru remedierea vulnerabilității (de exemplu, un link către un site Web cu o actualizare a sistemului de operare sau o corecție de aplicație).
- Link către un site Web cu o descriere a vulnerabilității.

5. Pentru a vedea o descriere detaliată a vulnerabilității, fă clic pe linkul **Informații suplimentare** pentru a deschide o pagină Web cu o descriere a amenințării care este asociată cu vulnerabilitatea selectată. Site-ul Web [www.secunia.com](https://www.secunia.com)  îți permite să descarci și să instalezi actualizarea necesară pentru versiunea curentă a aplicației.

6. Selectează unul dintre următoarele moduri pentru a remedia o vulnerabilitate:



- Dacă pentru aplicație sunt disponibile una sau mai multe corecții, instalează corecția necesară urmând instrucțiunile furnizate lângă numele corecției.
- Dacă este disponibilă o actualizare de sistem de operare, instalează actualizarea necesară urmând instrucțiunile furnizate lângă numele actualizării.

Vulnerabilitatea este remediată după ce instalezi corecția sau actualizarea. Kaspersky Endpoint Security îi atribuie acestei vulnerabilități o stare care înseamnă că vulnerabilitatea a fost remediată. Înregistrarea despre vulnerabilitatea remediată este prezentată cu culoarea gri în lista de vulnerabilități.

7. Dacă în partea de jos a ferestrei nu sunt prezentate informații despre cum se remediază o vulnerabilitate, poți porni din nou activitatea Scanare de vulnerabilități după actualizarea bazei de date și a modulelor Kaspersky Endpoint Security. Deoarece Kaspersky Endpoint Security scanează sistemul după vulnerabilități cu o bază de date pentru vulnerabilități, după actualizarea aplicației este posibil să apară o înregistrare despre o vulnerabilitate remediată.

## Ascunderea înregistrărilor din lista de vulnerabilități

Poți ascunde o înregistrare de vulnerabilitate selectată. Kaspersky Endpoint Security atribuie starea *Ascuns* înregistrărilor selectate în lista de vulnerabilități și acestea sunt marcate ca ascunse. Apoi poți să [filtrezi lista de vulnerabilități după valoarea de stare \*Ascuns\*](#).

*Pentru a ascunde o înregistrare în lista de vulnerabilități:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Vulnerabilități**.

Fila **Vulnerabilități** conține o listă de vulnerabilități pe care Kaspersky Endpoint Security le-a detectat în cursul activității Scanare de vulnerabilități.

4. În lista de vulnerabilități, selectează înregistrarea pentru vulnerabilitatea pe care dorești s-o ascunzi.

În partea de jos a listei de vulnerabilități se deschide o secțiune cu informații despre această vulnerabilitate și recomandări pentru remedierea ei.

5. Fă clic pe butonul **Ascundere**.

Kaspersky Endpoint Security atribuie starea *Ascuns* vulnerabilității selectate. Înregistrările despre vulnerabilitățile cu starea *Ascuns* sunt mutate la sfârșitul listei de vulnerabilități și au culoarea gri.

6. Pentru a ascunde o înregistrare despre o vulnerabilitate în lista de vulnerabilități, bifează caseta de selectare **Ascuns** în partea de sus a listei.

## Filtrarea listei de vulnerabilități după nivelul de gravitate

*Pentru a filtra lista de vulnerabilități după nivelul de gravitate:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Vulnerabilități**.  
Fila **Vulnerabilități** conține o listă de vulnerabilități pe care Kaspersky Endpoint Security le-a detectat în cursul activității Scanare de vulnerabilități. În partea de sus a listei de vulnerabilități, în rândul **Afișare gravitate**, apar trei pictograme pentru nivelul de gravitate pentru vulnerabilitate (Avertizare, Important, Critic). Făcând clic pe aceste pictograme poți filtra lista de vulnerabilități după nivelul de gravitate.
4. Fă clic pe una, două sau trei pictograme pentru nivelul de gravitate pentru vulnerabilitate. În listă sunt afișate vulnerabilitățile care corespund nivelurilor de gravitate selectate. Pentru a opri afișarea în listă a vulnerabilităților care corespund unui anumit nivel de severitate, fă clic din nou pe pictograma nivelului de gravitate relevant. Dacă nu este selectat niciun nivel de gravitate, lista de vulnerabilități este goală.

Condițiile de filtrare pentru înregistrarea de vulnerabilitate selectată sunt salvate după ce închizi fereastra **Stocări**.

## Filtrarea listei de vulnerabilități după valorile de stare Remediat și Ascuns

*Pentru a filtra lista de vulnerabilități după valorile de stare Remediat și Ascuns:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.
3. În fereastra **Stocări**, selectează fila **Vulnerabilități**.  
Fila **Vulnerabilități** conține o listă de vulnerabilități pe care Kaspersky Endpoint Security le-a detectat în cursul activității Scanare de vulnerabilități.
4. Casetele de selectare care indică starea vulnerabilităților sunt prezentate lângă setarea **Afișare vulnerabilități**. Pentru a filtra lista de vulnerabilități după starea *Remediat*, procedează astfel:

- Pentru a afișa înregistrările despre vulnerabilitățile remediate din lista de vulnerabilități, bifează caseta de selectare **Remediat**. Înregistrările despre vulnerabilitățile remediate sunt colorate cu gri în lista de vulnerabilități.
- Pentru a ascunde înregistrările despre vulnerabilitățile remediate din lista de vulnerabilități, golește caseta de selectare **Remediat**.

5. Pentru a filtra lista de vulnerabilități după starea *Ascuns*, procedează astfel:

- Pentru a afișa înregistrările despre vulnerabilitățile ascunse din lista de vulnerabilități, bifează caseta de selectare **Ascuns**. Înregistrările despre vulnerabilitățile ascunse sunt colorate cu gri în lista de vulnerabilități.
- Pentru a ascunde înregistrările despre vulnerabilitățile ascunse din lista de vulnerabilități, golește caseta de selectare **Ascuns**.

Condițiile de filtrare pentru înregistrarea de vulnerabilitate selectată nu sunt salvate după ce închizi fereastra **Stocări**.

## Verificarea integrității modulelor aplicației

Această secțiune conține informații despre aspectele specifice și setările activității Verificare integritate.

## Despre activitatea Verificare integritate

Kaspersky Endpoint Security verifică modulele aplicației din directorul de instalare a aplicației pentru a vedea dacă sunt deteriorate sau modificate. Dacă un modul al aplicației are o semnătură digitală incorectă, modulul este considerat deteriorat.

După [pornirea activității Verificare integritate](#), progresul său este afișat în câmpul din dreptul numelui activității, în secțiunea **Activități** din fila **Protecție și control** a ferestrei principale a Kaspersky Endpoint Security.

Rezultatele activității Verificare integritate sunt înregistrare în [rapoarte](#).

## Pornirea și oprirea unei activități Verificare integritate

Indiferent de modul de executare selectat, poți porni sau opri oricând o activitate de verificare a integrității.

*Pentru a porni sau a opri o activitate de verificare a integrității:*

1. Deschide [fereastra principală a aplicației](#).
2. Selectează fila **Protecție și control**.
3. Deschide secțiunea **Activități**.
4. Fă clic dreapta pentru a afișa meniul contextual corespunzător liniei cu numele activității de verificare a integrității.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a porni activitate Verificare integritate, selectează **Pornire scanare** din meniu.  
Starea progresului activității afișată în dreapta butonului cu numele acestei activități se modifică în *Se execută*.
  - Dacă dorești să oprești activitatea de verificare a integrității, selectează **Oprire scanare** din meniul contextual.  
Starea progresului activității afișată în dreapta butonului cu numele acestei activități se modifică în *Oprită*.

## Selectarea modului de executare pentru activitatea de verificare a integrității

*Pentru a selecta modul de executare pentru activitatea de verificare a integrității:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Activități planificate**, selectează **Verificare integritate**.  
În partea dreaptă a ferestrei sunt afișate setările pentru activitatea Verificare integritate.
3. În secțiunea **Mod executare**, selectează una dintre următoarele opțiuni:
  - Dacă dorești să pornești manual activitatea Verificare integritate, selectează **Manual**.
  - Dacă dorești să configurezi o planificare de pornire a activității Verificare integritate, selectează **După planificare**.
4. Dacă la pasul anterior ai selectat opțiunea **După planificare**, specifică setările pentru planificarea executării activității. Pentru aceasta:
  - a. În lista verticală **Frecvență**, specifică momentul pornirii activității Verificare integritate. Selectează una dintre opțiunile următoare: **Minute**, **Ore**, **Zile**, **Săptămânal**, **La o oră specificată**, **Lunar** sau **După pornirea aplicației**.

- b. În funcție de elementul selectat în lista verticală **Frecvență**, specifică valoarea pentru setările care definesc ora pornirii activității.
- c. Dacă dorești ca aplicația Kaspersky Endpoint Security să pornească activitățile Verificare integritate omise cât mai curând posibil, bifează caseta de selectare **Executare activități omise**.

Dacă selectezi **După pornirea aplicației**, **Minute** sau **Ore** în lista verticală **Frecvență**, caseta de selectare **Executare activități omise** este indisponibilă.

- d. Dacă dorești ca aplicația Kaspersky Endpoint Security să suspende o activitate atunci când resursele computerului sunt limitate, bifează caseta de selectare **Execută doar atunci când computerul este inactiv**.

Această opțiune de planificare ajută la conservarea resurselor computerului.

5. Fă clic pe **OK**.


6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Gestionarea rapoartelor

Această secțiune prezintă modul în care poți configura setările pentru rapoarte și gestiona rapoartele.

## Principiile gestionării rapoartelor

Informațiile despre funcționarea fiecărei componente Kaspersky Endpoint Security, performanțele fiecărei activități de scanare, de actualizare, de controlare a integrității și de scanare de vulnerabilități, precum și funcționarea generală a aplicației sunt înregistrate în rapoarte.




Datele din raport sunt prezentate sub forma unui tabel care conține o listă de evenimente. Fiecare rând din tabel conține informații despre un eveniment separat. Atributele de eveniment sunt localizate în coloanele tabelului. Anumite coloane sunt compuse și conțin coloane imbricate, cu atribute suplimentare. Pentru a vizualiza atribute suplimentare, trebuie să faci clic pe butonul  lângă numele graficului. Evenimentele care sunt înregistrate în jurnal în timpul funcționării diferitelor componente sau performanțele diferitelor activități au seturi diferite de atribute.

Sunt disponibile următoarele rapoarte:

- Raport **Auditare sistem**. Conține informații despre evenimente apărute în cursul interacțiunii dintre utilizator și aplicație și în cursul funcționării aplicației în general, care nu sunt legate de nicio componentă sau activitate particulară a Kaspersky Endpoint Security.

- Raportul **Toate componentele protecției**. Conține informații despre evenimentele înregistrate în jurnal pe parcursul funcționării următoarelor componente ale aplicației Kaspersky Endpoint Security:
  - Antivirus pentru fișiere
  - Antivirus pentru e-mail.
  - Antivirus pentru Web.
  - Antivirus IM.
  - Monitorizare sistem.
  - Firewall.
  - Blocare atacuri de rețea.
  - Prevenire atac BadUSB.
- Raport privind funcționarea unei componente sau privind excluderea unei activități Kaspersky Endpoint Security.
- Raport **Criptare**. Conține informații despre evenimente apărute în cursul criptării sau decriptării datelor.

Rapoartele folosesc următoarele nivele de importanță pentru evenimente:

- **Evenimente informaționale**. Pictogramă . Evenimente formale care nu conțin de regulă informații importante.
- **Evenimente importante**. Pictogramă . Evenimente care solicită atenție, deoarece ele reflectă situații importante în funcționarea Kaspersky Endpoint Security.
- **Evenimente critice**. Pictogramă . Evenimente de importanță critică indicând probleme în funcționarea Kaspersky Endpoint Security sau vulnerabilități în protecția computerului utilizatorului.

Pentru o procesare convenabilă a rapoartelor, poți modifica prezentarea datelor pe ecran în modurile următoare:

- Filtrare listă de evenimente după diferite criterii.
- Utilizare funcție de căutare pentru a găsi un anumit eveniment.
- Vizualizare eveniment selectat într-o secțiune separată.

- Sortare listă de evenimente după fiecare coloană a raportului.
- Afișare și ascundere evenimente grupate de filtrul de evenimente.
- Modificare ordine și aranjare coloane prezentate în raport.

Poți salva un raport generat într-un fișier text, dacă este necesar.

De asemenea, poți [șterge informații de raport](#) privind componentele și activitățile Kaspersky Endpoint Security care sunt combinate în grupuri. Kaspersky Endpoint Security șterge toate înregistrările din rapoartele selectate, de la prima înregistrare cronologică până la ora curentă.

## Configurarea setărilor pentru rapoarte

Poți configura zona pentru rapoarte în următoarele moduri:

- Configurează durata maximă de stocare a rapoartelor.

Durata maximă implicită de stocare pentru rapoartele despre evenimentele înregistrate în jurnal de Kaspersky Endpoint Security este de 30 de zile. După această perioadă de timp, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport. Poți revoca restricția bazată pe timp sau poți modifica durata maximă de stocare a rapoartelor.

- Configurează dimensiunea maximă a fișierului raport.

Poți specifica dimensiunea maximă a fișierului care conține raportul. În mod implicit, dimensiunea maximă a fișierului raport este de 1.024 MB. Pentru a evita depășirea dimensiunii maxime a fișierului raport, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport atunci când este atinsă dimensiunea maximă a acestuia. Poți revoca restricția privind dimensiunea fișierului raport sau poți seta o altă valoare.

## Configurarea duratei maxime de stocare a rapoartelor

*Pentru a modifica durata maximă de stocare a fișierelor:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.
3. În partea dreaptă a ferestrei, în secțiunea **Parametri raport**, execută una dintre următoarele acțiuni:
  - Pentru a limita durata de stocare a rapoartelor, bifează caseta de selectare **Stocare rapoarte nu mai mult de**. În câmpul de lângă caseta de selectare **Stocare rapoarte nu mai mult de**, specifică durata maximă de stocare a rapoartelor.

Durata maximă implicită de stocare pentru rapoarte este de 30 de zile.

- Pentru a revoca limita privind durata de stocare a rapoartelor, debifează caseta de selectare **Stocare rapoarte nu mai mult de**.

Limita pentru durata de stocare a rapoartelor este activată în mod implicit.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea dimensiunii maxime a fișierului raport

*Pentru a configura dimensiunea maximă a fișierului raport:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.
3. În partea dreaptă a ferestrei, în secțiunea **Parametri raport**, efectuează una dintre următoarele acțiuni:
  - Pentru a limita dimensiunea fișierului raport, bifează caseta de selectare **Dimensiune maximă fișier**. În câmpul din dreapta casetei de selectare **Dimensiune maximă fișier**, specifică dimensiunea maximă a fișierului raport.

În mod implicit, dimensiunea fișierului de raport este limitată la 1.024 MB.

- Pentru a elimina restricția pentru dimensiunea fișierului raport, debifează caseta de selectare **Dimensiune maximă fișier**.

În mod implicit, limita pentru dimensiunea fișierului de raport este activată.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Vizualizarea rapoartelor

*Pentru a vizualiza rapoarte:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Rapoarte** pentru a deschide fereastra **Rapoarte**.
3. Pentru a genera un raport Toate componentele protecției, în stânga ferestrei **Rapoarte**, selectează elementul **Toate componentele protecției** în lista de componente și activități.

Raportul Toate componentele protecției se afișează în partea dreaptă a ferestrei și conține o listă de evenimente apărute în funcționarea tuturor componentelor de protecție ale Kaspersky Endpoint Security.



4. Pentru a genera un raport privind funcționarea unei componente sau a unei activități, în stânga ferestrei **Rapoarte**, în lista de componente și activități, selectează o componentă sau o activitate.

Un raport se afișează în partea dreaptă a ferestrei și conține o listă de evenimente apărute în funcționarea componentei sau activității Kaspersky Endpoint Security selectate.

În mod implicit, evenimentele din raport sunt sortate în ordinea crescătoare a valorilor din coloana **Data eveniment**.

## Vizualizarea informațiilor despre eveniment în raport

Poți vedea un sumar detaliat pentru fiecare eveniment în raport.

*Pentru a vedea un sumar detaliat pentru un eveniment în raport:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Rapoarte** pentru a deschide fereastra **Rapoarte**.
3. În stânga ferestrei, selectează raportul relevant pentru componentă sau activitate.  
Evenimentele incluse în domeniul raportului sunt afișate în tabelul din dreapta ferestrei. Pentru a găsi evenimente specifice în raport, folosește funcțiile de filtrare, căutare și sortare.
4. Selectează evenimentul relevant în raport.

În partea de jos a ferestrei este afișată o secțiune din sumarul evenimentului.

## Salvarea unui raport într-un fișier

Rapoartele pe care le generezi pot fi salvate în fișiere în format text (TXT) sau în fișiere CSV.

Kaspersky Endpoint Security înregistrează evenimentele în raport în același mod în care acestea sunt afișate pe ecran: cu alte cuvinte, cu același set și aceeași secvență de atribute de evenimente.

*Pentru a salva un raport într-un fișier:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Rapoarte** pentru a deschide fereastra **Rapoarte**.

### 3. Efectuează una dintre următoarele acțiuni:

- Pentru a genera raportul protecției generale, selectează **Toate componentele protecției** în lista de componente și de activități.

Raportul „Toate componentele protecției” se afișează în partea dreaptă a ferestrei și conține o listă de evenimente apărute în funcționarea tuturor componentelor de protecție.

- Pentru a genera un raport privind funcționarea unei anumite componente sau activități, selectează componenta sau activitatea respectivă în lista de componente și activități.

Raportul se afișează în partea dreaptă a ferestrei și conține o listă de evenimente apărute în funcționarea componentei sau activității selectate.

### 4. Dacă este necesar, poți modifica prezentarea datelor în raport:

- Filtrând evenimentele
- Executând o căutare de eveniment
- Rearanjând coloanele
- Sortând evenimentele

### 5. Fă clic pe butonul **Salvare raport** în partea din dreapta sus a ferestrei.

Se deschide un meniu contextual.

### 6. În meniul contextual, selectează codificarea pentru salvarea fișierului de raport: **Salvare ca ANSI** sau **Salvare ca Unicode**.

Se deschide fereastra standard Microsoft Windows **Save as (Salvare ca)**.

### 7. În fereastra **Save as (Salvare ca)**, specifică directorul destinație pentru fișierul de raport.

### 8. În câmpul **Nume fișier**, tastează numele de fișier al raportului.

### 9. În câmpul **Tip fișier**, selectează formatul de fișier de raport necesar: TXT sau CSV.

### 10. Fă clic pe butonul **Salvare**.

## Golirea rapoartelor

*Pentru a elimina informații din rapoarte:*

### 1. Deschide [fereastra cu setările aplicației](#).

### 2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

3. În partea dreaptă a ferestrei, în secțiunea **Parametri raport**, fă clic pe butonul **Ștergere rapoarte**.

Se deschide fereastra **Golire rapoarte**.

4. Bifează casetele de selectare de lângă rapoartele din care dorești să ștergi informații:

- **Toate rapoartele.**
- **Raport protecție generală.** Conține informații despre funcționarea următoarelor componente ale aplicației Kaspersky Endpoint Security:
  - Antivirus pentru fișiere
  - Antivirus pentru e-mail.
  - Antivirus pentru Web.
  - Antivirus IM.
  - Monitorizare sistem.
  - Firewall.
  - Blocare atacuri de rețea.
  - Prevenire atac BadUSB.
- **Raport activități scanare.** Conține informații despre activitățile de scanare finalizate:
  - Scanarea completă
  - Scanarea zonelor critice
  - Scanarea particularizată
  - Verificare integritate.
- **Raport activități actualizare.** Conține informații despre activitățile de actualizare finalizate:
- **Raport Firewall.** Conține informații despre funcționarea componentei Firewall.
- **Raport Componente de control.** Conține informații despre funcționarea următoarelor componente ale aplicației Kaspersky Endpoint Security:
  - Componenta Control pornire aplicații.

- Componenta Control privilegii aplicației.
- Monitor de vulnerabilități.
- Componenta Control dispozitive.
- Control Web.
- **Raport Criptare date.**

5. Fă clic pe **OK**.

## Serviciul de notificare

Această secțiune conține informații despre serviciul de notificare care-l alertează pe utilizator cu privire la evenimentele care apar în funcționarea aplicației Kaspersky Endpoint Security, precum și instrucțiuni privind configurarea parametrilor pentru notificări.

## Despre notificările aplicației Kaspersky Endpoint Security

În timpul funcționării Kaspersky Endpoint Security apar tot felul de evenimente. Notificările referitoare la aceste evenimente pot fi pur informative sau pot conține informații critice. De exemplu, notificările se pot informa despre finalizarea cu succes a unei actualizări a bazei de date sau a unui modul al aplicației sau înregistrarea unor erori la componente care necesită remediere.

Kaspersky Endpoint Security acceptă înregistrarea în jurnal a informațiilor despre evenimente în funcționarea jurnalului de aplicații Microsoft Windows și/sau a jurnalului de evenimente Kaspersky Endpoint Security.

Kaspersky Endpoint Security furnizează notificări în următoarele moduri:

- utilizând notificări pop-up zona de notificare a barei de activități Microsoft Windows;
- prin e-mail.

Poți configura furnizarea notificărilor de evenimente. Metoda de furnizare a notificărilor este configurată pentru fiecare tip de eveniment.

## Configurarea serviciului de notificare

Poți efectua următoarele acțiuni pentru configurarea serviciului de notificări:

- Configurează setările jurnalelor de evenimente în care Kaspersky Endpoint Security înregistrează evenimentele.

- Configurează modul de afișare a notificărilor pe ecran.
- Configurează furnizarea notificărilor prin e-mail.

Atunci când folosești tabelul de evenimente pentru a configura serviciul de notificări, poți executa următoarele acțiuni:

- Filtrează evenimentele serviciului de notificări după valorile coloanei sau utilizând condiții de filtrare particularizate.
- Utilizează funcția de căutare pentru evenimentele serviciului de notificări.
- Sortează evenimentele serviciului de notificări.
- Schimbă ordinea și setul de coloane afișate în lista de evenimente ale serviciului de notificări.

## Configurarea setărilor pentru jurnalul de evenimente

*Pentru a configura setările jurnalului de evenimente:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

În partea dreaptă a ferestrei sunt afișate setările pentru rapoarte și zone de stocare.

3. În secțiunea **Notificări**, fă clic pe butonul **Setări**.

Această acțiune deschide fereastra **Notificări**.

Componentele și activitățile aplicației Kaspersky Endpoint Security se afișează în partea stângă a ferestrei. În partea dreaptă a ferestrei sunt prezentate evenimentele generate pentru componenta sau activitatea selectată.

4. În stânga ferestrei, selectează componenta sau activitatea pentru care dorești să configurezi setările jurnalului de evenimente.

5. Bifează casetele de selectare de lângă evenimentele relevante în coloane **Salvare în jurnal local** și **Salvare în Jurnal evenimente Windows**.

Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvare în jurnal local** sunt afișate în **Jurnale aplicații și servicii** în secțiunea **Jurnal de evenimente Kaspersky**.

Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvare în Jurnal evenimente Windows** sunt afișate în **Jurnale Windows** în secțiunea **Aplicație**. Pentru a deschide jurnalele de evenimente, fă clic pe **Start** → **Control Panel** → **Administration** → **Event Viewer**.

6. Fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea afișării și livrării notificărilor

*Pentru a configura afișarea și livrarea notificărilor:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

În partea dreaptă a ferestrei sunt afișate setările pentru rapoarte și zone de stocare.

3. În secțiunea **Notificări**, fă clic pe butonul **Setări**.

Această acțiune deschide fereastra **Notificări**.

Componentele și activitățile aplicației Kaspersky Endpoint Security se afișează în partea stângă a ferestrei. În partea dreaptă a ferestrei se listează evenimentele generate pentru componenta selectată sau pentru activitatea selectată.

4. În stânga ferestrei, selectează componenta sau activitatea pentru care dorești să configurezi furnizarea notificărilor.

5. În coloana **Notificare pe ecran**, bifează casetele de selectare de lângă evenimentele necesare.

Informațiile despre evenimentele selectate se vor afișa pe ecran ca mesaje pop-up în zona de notificare a barei de activități Microsoft Windows.

6. În coloana **Notificare prin e-mail**, bifează casetele de selectare de lângă evenimentele necesare.

Informațiile despre evenimentele selectate sunt livrate prin e-mail, dacă setările de livrare a notificărilor prin e-mail sunt configurate.

7. Fă clic pe butonul **Setări notificare e-mail**.

Această acțiune deschide fereastra **Setări notificare e-mail**.

8. Bifează caseta de selectare **Trimitere notificări despre evenimente** pentru a activa furnizarea de informații despre evenimentele Kaspersky Endpoint Security selectate în coloana **Notificare prin e-mail**.

9. Specifică setările de livrare a notificărilor prin e-mail.

10. Fă clic pe **OK**.



11. În fereastra **Setări notificare e-mail**, fă clic pe **OK**.

12. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Configurarea afișării avertizărilor despre starea aplicației în zona de notificare

*Pentru a configura afișarea avertizărilor despre starea aplicației în zona de notificare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Interfață**.  
Setările interfeței Kaspersky Endpoint Security sunt afișate în dreapta ferestrei.
3. În secțiunea **Avertizări**, bifează casetele de selectare de lângă categoriile de evenimente despre care dorești să vezi notificări în zona de notificare din Microsoft Windows.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Atunci când apar evenimente din categoria selectată, [pictograma aplicație](#) din zona de notificare se modifică în  sau în , în funcție de gravitatea avertizării.

## Gestionarea carantinei și a copiilor de rezervă

Această secțiune prezintă modul în care poți configura și gestiona carantina și copiele de rezervă.

## Despre carantină și copiele de rezervă

*Carantina* este o listă de fișiere probabil infectate. *Fișierele probabil infectate* sunt fișiere care ar putea conține viruși și alte amenințări sau varietăți ale acestor amenințări.

Atunci când Kaspersky Endpoint Security trimite în carantină un fișier potențial infectat, el nu copiază fișierul, ci îl mută: aplicația șterge fișierul de pe unitatea de hard disk sau din mesajul de e-mail și salvează fișierul într-un spațiu de stocare a datelor special. Fișierele din Carantină sunt salvate într-un format special și nu reprezintă o amenințare.

Kaspersky Endpoint Security poate detecta și trimite în carantină un fișier potențial infectat atunci când se execută [o scanare de viruși](#) și, de asemenea, în timpul funcționării componentelor [Antivirus pentru fișiere](#), [Antivirus pentru e-mail](#) și [Monitorizare sistem](#).

Kaspersky Endpoint Security plasează fișiere în Carantină în următoarele cazuri:

- Codul fișierului seamănă cu un program malware cunoscut, dar modificat parțial, sau are o structură asemănătoare unui malware, dar nu este listat în baza de date Kaspersky Endpoint Security. În acest caz, fișierul este plasat în Carantină după analiza euristică efectuată de Antivirus pentru fișiere și Antivirus pentru e-mail sau în cursul unei scanări de viruși. Analiza euristică rareori determină alarme false.

- Secvența de operațiuni pe care o execută un fișier este periculoasă. În acest caz, fișierul este plasat în Carantină după ce componenta Monitorizare sistem i-a analizat comportamentul.

*Copia de rezervă* este o listă de copii de rezervă care au fost șterse sau modificate în timpul procesului de dezinfectie. *Copia de rezervă* este o copie a fișierului creată la prima încercare de dezinfectare sau ștergere a acestui fișier. Copiile de rezervă ale fișierelor sunt stocate într-un format special și nu reprezintă o amenințare.

Uneori nu este posibilă păstrarea integrității fișierelor în timpul dezinfectării. Dacă după dezinfectare pierzi parțial sau total accesul la informații importante dintr-un fișier dezinfectat, poți încerca să restabilești copia dezinfectată în directorul inițial.

Este posibil ca, după altă actualizare a bazei de date sau a modulelor software ale aplicației, Kaspersky Endpoint Security să poată identifica definitiv amenințările și să le neutralizeze. Prin urmare, este recomandată scanarea fișierelor din carantină după fiecare actualizare a bazei de date sau a modulelor software ale aplicației.

## Configurarea setărilor pentru Carantină și Copie de rezervă

Zona de stocare este compusă din zonele Carantină și Copie de rezervă. Poți configura setările pentru Carantină și Copie de rezervă după cum urmează:

- Configurează durata maximă de stocare a fișierelor în Carantină și de stocare a copiilor de fișiere în Copie de rezervă.

Durata maximă implicită de stocare a fișierelor în Carantină și de stocare a copiilor de fișiere în Copie de rezervă este de 30 de zile. După ce durata maximă de stocare expiră, aplicația Kaspersky Endpoint Security șterge cele mai vechi fișiere din zona de stocare a datelor. Poți revoca restricția bazată pe timp sau poți modifica durata maximă de stocare a fișierelor.

- Poți configura dimensiunea maximă a zonelor Carantină și Copie de rezervă.

În mod implicit, dimensiunea maximă a zonelor Carantină și Copie de rezervă este de 100 MO. Atunci când se atinge limita zonei de stocare, aplicația Kaspersky Endpoint Security șterge automat cele mai vechi fișiere din zonele Carantină și Copie de rezervă, astfel încât dimensiunea maximă a zonei de stocare a datelor să nu fie depășită. Poți revoca limita de dimensiune pentru zonele Carantină și Copie de rezervă sau poți modifica dimensiunea lor maximă.

## Configurarea duratei maxime de stocare a fișierelor în Carantină și de stocare a copiilor de fișiere în Copie de rezervă

*Pentru a configura durata maxime de stocare a fișierelor în Carantină și de stocare a copiilor de fișiere în Copie de rezervă:*

1. Deschide [fereastra cu setările aplicației](#).



2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

3. Efectuează una dintre următoarele acțiuni:

- Pentru a limita durata de stocare a fișierelor în zonele Carantină și Copie de rezervă, în partea dreaptă a ferestrei, în secțiunea **Setări pentru carantină și copiere de siguranță**, bifează caseta de selectare **Stocare obiecte nu mai mult de**. În câmpul din dreapta casetei de selectare **Stocare obiecte nu mai mult de**, specifică durata maximă de stocare pentru fișierele din Carantină și copiile fișierelor din Copie de rezervă. Durata de stocare pentru fișierele din Carantină și copiile de fișiere din Copie de rezervă este limitată în mod implicit la 30 de zile.
- Pentru a anula limita pentru durata de stocare a fișierelor în zonele Carantină și Copie de rezervă, în partea dreaptă a ferestrei, în secțiunea **Setări pentru carantină și copiere de siguranță**, bifează caseta de selectare **Stocare obiecte nu mai mult de**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Configurarea dimensiunii maxime a zonelor Carantină și Copie de rezervă

*Pentru a configura dimensiunea maximă a zonelor Carantină și Copie de rezervă:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

3. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să limitezi dimensiunea totală pentru Carantină și Copie de rezervă, bifează caseta de selectare **Dimensiune maximă spațiu de stocare** în dreapta ferestrei, în secțiunea **Setări pentru carantină și copiere de siguranță**, și specifică dimensiunea maximă pentru Carantină și Copie de rezervă în câmpul din dreapta casetei de selectare **Dimensiune maximă spațiu de stocare**.

În mod implicit, dimensiunea maximă a spațiului de stocare pentru datele incluse în directorul Carantină și copiile de rezervă ale fișierelor este de 100 MO.

- Dacă dorești să elimini limita pentru dimensiunea totală pentru Carantină și Copie de rezervă, debifează caseta de selectare **Dimensiune maximă spațiu de stocare** în dreapta ferestrei, în secțiunea **Setări pentru carantină și copiere de siguranță**.

În mod implicit, dimensiunea pentru Carantină și Copie de rezervă nu este limitată.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Gestionarea zonei Carantină

Kaspersky Endpoint Security [șterge fișiere](#) în mod automat, indiferent de stare, din Carantină după expirarea duratei de stocare care este definită în setările aplicației.

La gestionarea zonei Carantină ai la dispoziție următoarele operațiuni pentru fișiere:

- Vizualizarea fișierelor mutate în carantină de aplicația Kaspersky Endpoint Security.
- Scanarea fișierelor probabil infectate utilizând versiunea curentă a bazelor de date și modulelor Kaspersky Endpoint Security.
- Restaurarea fișierelor din carantină în directoarele inițiale.
- Eliminarea fișierelor din carantină.
- Deschiderea directoarelor în care au fost amplasate inițial fișierele.

Lista fișierelor mutate în carantină este prezentată sub formă de tabel.

Poți efectua și următoarele acțiuni în timpul gestionării datelor din tabel:

- Filtrarea fișierelor introduse în Carantină după coloane și filtre particularizate.
- Utilizarea funcției de căutare a fișierelor mutate în carantină.
- Sortarea fișierelor mutate în carantină.
- Schimbarea ordinii și setarea coloanelor de afișat în tabelul de fișiere mutate în carantină.

Poți copia în clipboard evenimente selectate în Carantină. Pentru a selecta fișiere multiple plasate în Carantină, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

## Activarea și dezactivarea scanării fișierelor din carantină în urma unei actualizări

Dacă aplicația Kaspersky Endpoint Security detectează semne de infectare la scanarea unui fișier, dar nu poate stabili care anume programe periculoase l-au infectat, Kaspersky Endpoint Security mută fișierul respectiv în [Carantină](#). Kaspersky Endpoint Security poate identifica ulterior amenințarea, neutralizând-o după actualizarea bazelor de date și a modulelor aplicației. Poți activa scanarea automată a fișierelor din carantină în urma fiecărei actualizări a bazelor de date și modulelor aplicației.

Îți recomandăm să scanezi în mod regulat fișierele din carantină. Este posibil ca în urma scanării să se modifice starea fișierelor. Unele fișiere pot fi dezinfectate și restaurate în locațiile lor inițiale, astfel încât poți continua să le folosești.

*Pentru a activa scanarea fișierelor din carantină în urma actualizărilor:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează **Rapoarte și zone de stocare**.

În partea dreaptă a ferestrei se afișează setările de gestionare a rapoartelor și zonelor de stocare.

3. În secțiunea **Setări pentru carantină și copiere de siguranță**, efectuează una dintre următoarele acțiuni:

- Pentru a activa scanarea fișierelor din carantină în urma fiecărei actualizări a aplicației Kaspersky Endpoint Security, bifează caseta de selectare **Repetă scanarea fișierelor din Carantină după actualizare**.
- Pentru a dezactiva scanarea fișierelor din carantină în urma fiecărei actualizări a aplicației Kaspersky Endpoint Security, debifează caseta de selectare **Repetă scanarea fișierelor din Carantină după actualizare**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Pornirea unei activități de scanare particularizată pentru fișierele din carantină

După o actualizare a bazelor de date și a modulelor software ale aplicației, Kaspersky Endpoint Security poate identifica de o manieră definitivă amenințările din fișierele introduse în Carantină și le poate neutraliza. Dacă aplicația nu este configurată să scaneze fișierele introduse în Carantină în mod automat după fiecare actualizare a bazelor de date și a modulelor aplicației, poți porni manual o activitate Scanare particularizată pentru fișierele introduse în Carantină.

*Pentru a porni o activitate Scanare particularizată pentru fișierele din Carantină:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.

Se deschide fila **Carantină** din fereastra **Stocări**.

3. În fila **Carantină**, selectează unul sau mai multe fișiere probabil infectate pe care dorești să le scanezi.

Pentru a selecta fișiere multiple plasate în Carantină, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

4. Pornește activitatea de scanare particularizată într-unul din modurile următoare:

- Fă clic pe butonul **Repetare scanare**.
- Fă clic dreapta pentru a afișa meniul contextual și selectează **Repetare scanare**.

Atunci când scanarea este finalizată, apare o notificare cu numărul de fișiere scanate și numărul de amenințări detectate.

## Restaurarea fișierelor din carantină

*Pentru a restaura fișierele din Carantină:*

1. Deschide [fereastra principală a aplicației](#).
2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.  
Se deschide fila **Carantină** din fereastra **Stocări**.
3. Dacă dorești să restaurezi toate fișierele introduse în Carantină, selectează **Restaurare toate** în meniul contextual al oricărui fișier.  
Kaspersky Endpoint Security restaurează toate fișierele din Carantină în directoarele lor inițiale.
4. Pentru a restaura unul sau mai multe fișiere din carantină:

- a. În fila **Carantină**, selectează unul sau mai multe fișiere pe care dorești să le restaurezi din Carantină.

Pentru a selecta fișiere multiple plasate în Carantină, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

- b. Restaurează fișierele într-unul din modurile următoare:

- Fă clic pe butonul **Restaurare**.

- Fă clic dreapta pentru a deschide meniul contextual și selectează **Restaurare**.

Kaspersky Endpoint Security restaurează fișierele selectate în directoarele lor inițiale.

## Ștergerea fișierelor din carantină

*Pentru a șterge fișierele din Carantină:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.

Se deschide fila **Carantină** din fereastra **Stocări**.

3. Dacă dorești să ștergi toate fișierele din Carantină, selectează **Ștergere toate** în meniul contextual al oricărui fișier.

Kaspersky Endpoint Security șterge toate fișierele din Carantină.

4. Pentru a șterge unul sau mai multe fișiere din carantină:

a. În tabelul din fila **Carantină**, selectează unul sau mai multe fișiere probabil infectate pe care dorești să le ștergi din Carantină.

Pentru a selecta fișiere multiple plasate în Carantină, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le ștergi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

b. Șterge fișierele într-unul din modurile următoare:

- Fă clic pe butonul **Eliminare**.
- Fă clic dreapta pentru a deschide meniul contextual și selectează **Ștergere**.

Kaspersky Endpoint Security șterge fișierele selectate din Carantină.

## Gestionarea copiilor de rezervă

Dacă în fișier este detectat cod rău intenționat, Kaspersky Endpoint Security blochează fișierul, plasează o copie în Copie de rezervă și încearcă să-l dezinfecteze. Dacă dezinfectarea fișierului se face cu succes, starea copiei de rezervă a fișierului se modifică în *Dezinfectat*. Fișierul devine disponibil în directorul său original. Dacă un fișier nu poate fi dezinfectat, Kaspersky Endpoint Security îl șterge din directorul său original. Poți restaura fișierul din copia sa de rezervă în directorul său original.

Atunci când detectează cod rău intenționat într-un fișier care face parte din aplicația Windows Store, Kaspersky Endpoint Security șterge imediat fișierul, fără a-l muta în Copie de rezervă. Poți restaura integritatea aplicației Windows Store folosind instrumentele adecvate din sistemul de operare Microsoft Windows 8 (consultă *fișierele de ajutor Microsoft Windows 8* pentru detalii referitoare la restaurarea aplicației Windows Store).

Kaspersky Endpoint Security [șterge copiile de rezervă ale fișierelor](#) în mod automat din Copie de rezervă, indiferent de stare, după expirarea duratei de stocare definite în setările aplicației.

Poți, de asemenea, să ștergi manual orice copie a unui fișier din Copie de rezervă.

Setul de copii de rezervă ale fișierelor este prezentat sub formă de tabel.

În timpul gestionării Copiei de rezervă, poți efectua următoarele acțiuni cu copiile de rezervă ale fișierelor:

- Vizualizarea setului de copii de rezervă ale fișierelor.
- Restaurarea fișierelor din copiile de rezervă în directoarele inițiale.
- Ștergerea copiilor de rezervă ale fișierelor din Copie de rezervă.

Poți efectua și următoarele acțiuni în timpul gestionării datelor din tabel:

- Filtrarea copiilor de rezervă după coloane, inclusiv după condiții de filtrare particularizate.
- Utilizarea funcției de căutare a copiilor de rezervă.
- Sortarea copiilor de rezervă.
- Schimbarea ordinii și setarea coloanelor de afișat în tabelul de copii de rezervă.

Poți copia în clipboard evenimente de Copie de rezervă selectate. Pentru a selecta fișiere copie de rezervă multiple, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

## Restaurarea fișierelor din Copie de rezervă

*Pentru a restaura fișierele din Copie de rezervă:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.

3. În fereastra **Stocări**, selectează fila **Copie de rezervă**.

4. Dacă dorești să restaurezi toate fișierele din Copie de rezervă, selectează **Restaurare toate** în meniul contextual al oricărui fișier.

Kaspersky Endpoint Security restaurează toate fișierele din copiile lor de rezervă în directoarele lor inițiale.

5. Pentru a restaura unul sau mai multe fișiere din Copie de rezervă:

a. În fila **Copie de rezervă** din tabel, selectează unul sau mai multe fișiere copie de rezervă.

Pentru a selecta fișiere multiple plasate în Carantină, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

b. Restaurează fișierele într-unul din modurile următoare:

- Fă clic pe butonul **Restaurare**.
- Fă clic dreapta pentru a deschide meniul contextual și selectează **Restaurare**.

Kaspersky Endpoint Security restaurează toate fișierele din copiile de rezervă selectate în directoarele lor inițiale.

## Ștergerea copiilor de rezervă ale fișierelor din Copie de rezervă

*Pentru a șterge copiile de rezervă ale fișierelor din Copie de rezervă:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea de sus a ferestrei principale a aplicației, fă clic pe linkul **Carantină** pentru a deschide fereastra **Stocări**.

3. În fereastra **Stocări**, selectează fila **Copie de rezervă**.

4. Dacă dorești să ștergi toate fișierele din Copie de rezervă, efectuează una dintre următoarele acțiuni:

- În meniul contextual al oricărui fișier, selectează **Ștergere toate**.
- Fă clic pe butonul **Golire spațiu de stocare**.

Kaspersky Endpoint Security șterge toate copiile de rezervă ale fișierelor din Copie de rezervă.

## 5. Dacă dorești să ștergi unul sau mai multe fișiere din Copie de rezervă:

a. În fila **Copie de rezervă** din tabel, selectează unul sau mai multe fișiere copie de rezervă.

Pentru a selecta fișiere copie de rezervă multiple, fă clic dreapta pentru a deschide meniul contextual al oricărui fișier și selectează **Selectare totală**. Pentru a anula selectarea fișierelor pe care nu dorești să le scanezi, fă clic pe ele în timp ce ții apăsată tasta **CTRL**.

b. Șterge fișierele într-unul din modurile următoare:

- Fă clic pe butonul **Eliminare**.
- Fă clic dreapta pentru a deschide meniul contextual și selectează **Ștergere**.

Kaspersky Endpoint Security șterge copiile de rezervă selectate ale fișierelor din Copie de rezervă.

## Setările avansate ale aplicației

Această secțiune prezintă setările avansate ale aplicației Kaspersky Endpoint Security și modul de configurare a acestora.

## Crearea și folosirea unui fișier de configurare

Un fișier de configurare cu setări Kaspersky Endpoint Security îți permite să realizezi următoarele activități:

- Executarea instalării locale a Kaspersky Endpoint Security din linie de comandă, cu setări predefinite.  
Pentru aceasta, trebuie să salvezi fișierul de configurare în același director în care se găsește kitul de distribuție.
- Efectuarea instalării la distanță a Kaspersky Endpoint Security, prin intermediul Kaspersky Security Center, cu setări predefinite.
- Migrarea setărilor Kaspersky Endpoint Security de pe un computer pe altul.

*Pentru a crea un fișier de configurare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.
3. În secțiunea **Gestionare setări**, fă clic pe butonul **Salvare**.



Se deschide fereastra standard **Selectează un fișier de configurare** din Microsoft Windows.

4. Specifică o cale în care dorești să salvezi fișierul de configurare și introdu numele său.

Pentru a folosi fișierul de configurare pentru instalare locală sau la distanță a Kaspersky Endpoint Security, numele trebuie să fie `install.cfg`.

5. Fă clic pe butonul **Salvare**.

*Pentru a importa setările Kaspersky Endpoint Security dintr-un fișier de configurare:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.
3. În secțiunea **Gestionare setări**, fă clic pe butonul **Încărcare**.

Se deschide fereastra standard **Selectează un fișier de configurare** din Microsoft Windows.

4. Introdu calea către fișierul de configurare.
5. Fă clic pe butonul **Open** (Deschidere).

Toate valorile setărilor Kaspersky Endpoint Security vor fi setate conform fișierului de configurare selectat.

## Zona de încredere

Această secțiune conține informații despre zona de încredere și instrucțiuni despre configurarea excluderilor de la scanare și crearea unei liste de aplicații de încredere.

## Despre zona de încredere

O *zonă de încredere* este o listă de obiecte și aplicații configurate de administratorul de sistem, pe care Kaspersky Endpoint Security nu le monitorizează când este activ. Cu alte cuvinte, este o listă de excluderi de la scanare.


Administratorul formează zona de încredere independent, luând în considerare caracteristicile obiectelor gestionate și aplicațiile instalate pe computer. Este posibil să fie necesară includerea obiectelor și aplicațiilor în zona de încredere când Kaspersky Endpoint Security blochează accesul la un anumit obiect sau la o anumită aplicație, dacă ești sigur că obiectul sau aplicația respectivă este inofensivă.

Poți exclude următoarele obiecte de la scanare:

- Fișiere cu anumite formate
- Fișiere care sunt selectate de o mască
- Fișiere selectate
- Directoare
- Procese de aplicație

## Excluderi de la scanare

O *excludere de la scanare* este un set de condiții conform cărora Kaspersky Endpoint Security nu scanează un obiect după viruși și alte amenințări.

Excluderile de la scanare fac posibilă utilizarea în siguranță a software-urilor legitime care pot fi exploatate de infractori pentru a aduce daune computerului sau datelor personale. Cu toate că nu au funcții rău intenționate, astfel de aplicații pot fi utilizate drept componente auxiliare în programe malware. Exemple de astfel de aplicații includ instrumente de administrare de la distanță, clienți IRC, servere FTP, diverse utilitare pentru suspendarea sau ascunderea proceselor, înregistratoare de taste, spărgătoare de parole și programe de apelare automată. Aceste aplicații nu sunt clasificate drept viruși. Detalii privind software-ul legal care poate fi folosit de infractori pentru a aduce daune computerului sau datelor personale sunt disponibile la Enciclopedia de viruși Kaspersky la adresa <https://encyclopedia.kaspersky.com/knowledge/riskware/> .

Este posibil ca programul Kaspersky Endpoint Security să blocheze astfel de aplicații. Pentru a împiedica blocarea lor, poți configura excluderi de la scanare pentru aplicațiile în uz. În acest scop, adaugă numele sau masca de nume listată în Enciclopedia de viruși Kaspersky la zona de încredere. De exemplu, este posibil să utilizezi frecvent programul Remote Administrator. Acesta este o aplicație de acces de la distanță, care îți oferă controlul asupra unui computer aflat la distanță. Kaspersky Endpoint Security privește această activitate ca suspectă și este posibil să o blocheze. Pentru a împiedica blocarea aplicației, creează o excludere de la scanare cu numele sau masca de nume listată în Enciclopedia de viruși Kaspersky.

Dacă pe computerul tău este instalată o aplicație care colecționează informații și le trimite pentru a fi procesate, Kaspersky Endpoint Security este posibil să clasifice această aplicație drept malware. Pentru a evita acest lucru, poți exclude aplicația de la scanare configurând Kaspersky Endpoint Security așa cum este descris în acest document.

Excluderile de la scanare pot fi utilizate de următoarele componente și acțiuni ale aplicației, care sunt configurate de către administratorul de sistem:

- Antivirus pentru fișiere

- Antivirus pentru e-mail.
- Antivirus pentru Web.
- Componenta Control privilegii aplicații.
- Activități de scanare
- Monitorizare sistem.

## Lista aplicațiilor de încredere

*Lista de aplicații de încredere* este o listă de aplicații pentru care Kaspersky Endpoint Security nu monitorizează activitatea cu fișierele și activitatea în rețea (inclusiv activitatea rău intenționată) și nici accesul la registrul de sistem. În mod implicit, Kaspersky Endpoint Security scanează obiectele care sunt deschise, executate sau salvate de orice proces al unui program și controlează activitatea tuturor aplicațiilor și traficul în rețea generat de acestea. Kaspersky Endpoint Security exclude de la scanare aplicațiile din [lista de aplicații de încredere](#).

De exemplu, dacă presupui obiectele utilizate de aplicația Microsoft Windows Notepad standard ca fiind sigure fără scanare, ceea ce înseamnă că ai încredere în această aplicație, poți adăuga Microsoft Windows Notepad în lista de aplicații de încredere. Scanarea va omite atunci obiectele utilizate de această aplicație.

În plus, anumite acțiuni care sunt clasificate de către Kaspersky Endpoint Security ca fiind suspecte este posibil să fie sigure în contextul operațional pentru o serie de aplicații. De exemplu, interceptarea textului introdus de la tastatură este un proces de rutină pentru programele de comutare automată a structurii tastaturii (cum ar fi Punto Switcher). Pentru a ține cont de caracteristicile specifice ale unor astfel de aplicații și pentru a exclude activitatea lor din monitorizare, îți recomandăm să adaugi aceste aplicații în lista de aplicații de încredere.

Excluderea aplicațiilor de încredere din scanare permite evitarea conflictelor de compatibilitate dintre Kaspersky Endpoint Security și alte programe (de exemplu, problema scanării duble a traficului de rețea al unui computer terț de către Kaspersky Endpoint Security și de altă aplicație antivirus), crescând astfel performanțele computerului, aspect critic în cazul utilizării aplicațiilor server.

În același timp, fișierul executabil și procesele aplicației de încredere sunt scanate în continuare după viruși și alte programe malware. O aplicație poate fi exclusă complet din scanarea Kaspersky Endpoint Security cu ajutorul excluderilor de la scanare.

## Crearea unei excluderi de la scanare

Kaspersky Endpoint Security nu scanează un obiect dacă unitatea sau directorul care conține acel obiect este inclus(ă) în domeniul de scanare la începutul uneia dintre activitățile de scanare. Cu toate acestea, excluderea de la scanare nu se aplică atunci când se pornește o activitate de scanare particularizată pentru acest obiect particular.

*Pentru a crea o excludere de la scanare:*

1. Deschide [fereastra cu setările aplicației](#).

2. Selectează secțiunea **Protecție antivirus** din stânga.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.

Se deschide fereastra **Zonă de încredere** în fila **Excluderi de la scanare**.

4. Fă clic pe butonul **Adăugare**.

Se deschide fereastra **Excluderi de la scanare**. În această fereastră poți crea o excludere de la scanare folosind unul sau ambele criterii din secțiunea **Proprietăți**.

5. Pentru a exclude un fișier sau un director de la scanare:

a. În secțiunea **Proprietăți**, bifează caseta de selectare **Fișier sau director**.

b. Fă clic pe linkul **Selectare fișier sau director** din secțiunea **Descriere excludere de la scanare** pentru a deschide fereastra **Nume al fișierului sau al directorului**.

c. Introdu numele fișierului sau al directorului sau masca de nume pentru fișier sau director sau selectează fișierul sau directorul în arborele de directoare făcând clic pe **Răsfoire**.

În masca de nume a unui fișier sau a unui director, poți folosi caracterul asterisc (\*) pentru a înlocui orice set de caractere din numele fișierului.

De exemplu, poți folosi măști pentru a adăuga următoarele căi:

- Căi către fișiere aflate în orice director:
  - Masca „\*.exe” va include toate căile către fișierele care au extensia EXE.
  - Masca „test” va include toate căile către fișierele denumite „test”.
- Căi către fișierele aflate într-un director specificat:
  - Masca „C:\dir\\*.\*” va include toate căile către fișierele aflate în directorul C:\dir\, dar nu în subdirectoarele directorului C:\dir\.

- Masca „C:\dir\\*” va include toate căile către fișierele aflate în directorul C:\dir\, dar nu în subdirectoarele directorului C:\dir\.
- Masca „C:\dir\” va include toate căile către fișierele aflate în directorul C:\dir\, dar nu în subdirectoarele directorului C:\dir\.
- Masca „C:\dir\\*.exe” va include toate căile către fișierele cu extensia EXE aflate în directorul C:\dir\, dar nu în subdirectoarele directorului C:\dir\.
- Masca „C:\dir\test” va include toate căile către fișierele denumite „test” aflate în directorul C:\dir\, dar nu în subdirectoarele directorului C:\dir\.
- Masca „C:\dir\test” va include toate căile către fișierele denumite „test” aflate în directorul C:\dir\ și în subdirectoarele directorului C:\dir\.
- Căi către fișierele aflate în toate directoarele cu un nume specificat:
  - Masca „dir\\*.” va include toate căile către fișierele din directoarele denumite „dir”, dar nu în subdirectoarele acelor directoare.
  - Masca „dir\\*” va include toate căile către fișierele din directoarele denumite „dir”, dar nu în subdirectoarele acelor directoare.
  - Masca „dir\” va include toate căile către fișierele din directoarele denumite „dir”, dar nu în subdirectoarele acelor directoare.
  - Masca „dir\\*.exe” va include toate căile către fișierele cu extensia EXE din directoarele denumite „dir”, dar nu în subdirectoarele acelor directoare.
  - Masca „dir\test” va include toate căile către fișierele denumite „test” din directoarele denumite „dir”, dar nu în subdirectoarele acelor directoare.

d. În fereastra **Nume al fișierului sau al directorului**, fă clic pe **OK**.

În secțiunea **Descriere excludere de la scanare** din fereastra **Excluderi de la scanare** apare un link către fișierul sau directorul adăugat.

6. Pentru a exclude de la scanare obiecte cu un anumit nume:

a. În secțiunea **Proprietăți**, bifează caseta de selectare **Nume obiect**.

b. Fă clic pe linkul **Introducere nume obiect** în secțiunea **Descriere excludere de la scanare** pentru a deschide fereastra **Nume obiect**.

c. Introdu numele obiectului sau masca de nume în conformitate cu clasificarea din Enciclopedia de viruși Kaspersky:

d. Fă clic pe **OK** în fereastra **Nume obiect**.

În secțiunea **Descriere excludere de la scanare** din fereastra **Excluderi de la scanare** apare un link către numele obiectului.

7. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

8. Specifică apoi componentele aplicației Kaspersky Endpoint Security care trebuie să utilizeze excluderea de la scanare:

a. Dacă faci clic pe linkul **oricare** din secțiunea **Descriere excludere de la scanare** pentru a activa linkul **Selectare componente**.

b. Fă clic pe linkul **Selectare componente** pentru a deschide fereastra **Componente protecție**.

c. Bifează casetele de selectare de lângă componentele pentru care trebuie aplicată excluderea de la scanare.

d. În fereastra **Componente protecție**, fă clic pe **OK**.

În cazul în care componentele sunt specificate în setările pentru excluderea de la scanare, această excludere se aplică numai pentru scanarea de către aceste componente ale aplicației Kaspersky Endpoint Security.

În cazul în care componentele nu sunt specificate în setările excluderii de la scanare, această excludere se aplică pentru scanarea de către toate componentele aplicației Kaspersky Endpoint Security.

9. În fereastra **Excluderi de la scanare**, fă clic pe **OK**.

Excluderea de la scanare adăugată apare în fila **Excluderi de la scanare** din fereastra **Zonă de încredere**. Setările configurate pentru această excludere de la scanare apar în secțiunea **Descriere excludere de la scanare**.

10. În fereastra **Zonă de încredere**, fă clic pe **OK**.

11. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Modificarea unei excluderi de la scanare

*Pentru a modifica o excludere de la scanare:*

1. Deschide [fereastra cu setările aplicației](#).

2. Selectează secțiunea **Protecție antivirus** din stânga.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.

Se deschide fereastra **Zonă de încredere** în fila **Excluderi de la scanare**.

4. Selectează în listă excluderea de la scanare pe care dorești s-o modifice.

5. Modifică setările excluderii de la scanare folosind una dintre metodele următoare:

- Fă clic pe butonul **Editare**.

Se deschide fereastra **Excluderi de la scanare**.

- Deschide fereastra pentru editarea setării necesare făcând clic pe linkul din câmpul **Descriere excludere de la scanare**.

6. Dacă ai făcut clic pe butonul **Editare** la pasul precedent, fă clic pe **OK** în fereastra **Excluderi de la scanare**.

Setările modificate pentru această excludere de la scanare apar în secțiunea **Descriere excludere de la scanare**.

7. În fereastra **Zonă de încredere**, fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Ștergerea unei excluderi de la scanare

*Pentru a șterge o excludere de la scanare:*

1. Deschide [fereastra cu setările aplicației](#).

2. Selectează secțiunea **Protecție antivirus** din stânga.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.

Se deschide fereastra **Zonă de încredere** în fila **Excluderi de la scanare**.

4. Selectează excluderea de la scanare de care ai nevoie în lista de excluderi de la scanare.

5. Fă clic pe butonul **Eliminare**.

Excluderea de la scanare ștersă dispăre din listă.

6. În fereastra **Zonă de încredere**, fă clic pe **OK**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

# Activarea și dezactivarea unei excluderi de la scanare

*Pentru a activa și a dezactiva o excludere de la scanare:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Protecție antivirus** din stânga.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Zonă de încredere** în fila **Excluderi de la scanare**.
4. Selectează excluderea de care ai nevoie în lista de excluderi de la scanare.
5. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa o excludere de la scanare, bifează caseta de selectare de lângă acestei excluderi de la scanare.
  - Pentru a dezactiva o excludere de la scanare, debifează caseta de selectare de lângă numele acestei excluderi de la scanare.
6. Fă clic pe **OK**.
7. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Editarea listei de aplicații de încredere

*Pentru a edita lista de aplicații de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Protecție antivirus** din stânga.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Zonă de încredere**.
4. În fereastra **Zonă de încredere**, selectează fila **Aplicații de încredere**.
5. Pentru a adăuga o aplicație la lista de aplicații de încredere:
  - a. Fă clic pe butonul **Adăugare**.



b. În meniul contextual care se deschide, efectuează una dintre următoarele acțiuni:

- Dacă dorești să găsești aplicația în lista de aplicații instalate pe computer, selectează elementul **Aplicații** în meniu.

Se deschide fereastra **Selectare aplicația**.

- Dacă dorești să specifice calea către fișierul executabil al aplicației relevante, selectează **Răsfoire**.

Se deschide fereastra Microsoft Windows standard **Deschidere fișier** (Deschidere fișier).

c. Selectează aplicația într-unul din modurile următoare:

- Dacă ai selectat **Aplicații** la pasul precedent, selectează aplicația în lista de aplicații instalate pe computer și fă clic pe **OK** în fereastra **Selectare aplicația**.
- Dacă ai selectat **Răsfoire** la pasul precedent, specifică o cale către fișierul executabil al aplicației relevante și fă clic pe butonul **Deschis** în fereastra standard **Deschis** din Microsoft Windows.

Aceste acțiuni determină deschiderea ferestrei **Excluderi de la scanare pentru aplicație**.

a. Bifează casetele de selectare de lângă regulile pentru zone de încredere relevante pentru aplicația selectată:

- **Nu scana fișiere deschise.**
- **Nu monitoriza activitatea aplicației.**
- **Nu moșteni restricții de la procesul părinte (aplicație).**
- **Nu monitoriza activitatea aplicației subordonate.**
- **Nu se blochează interacțiunea cu interfața aplicației.**
- **Nu scana traficul de rețea.**

b. În fereastra **Excluderi de la scanare pentru aplicație**, fă clic pe **OK**.

Aplicația de încredere pe care ai adăugat-o apare în lista de aplicații de încredere.

6. Pentru a edita setările pentru o aplicație de încredere:

a. Selectează o aplicație din lista de aplicații de încredere.

b. Fă clic pe butonul **Editare**.

c. Se deschide fereastra **Excluderi de la scanare pentru aplicație**.

d. Bifează sau debifează casetele de selectare de lângă regulile pentru zone de încredere relevante pentru aplicația selectată:

Dacă în fereastra **Excluderi de la scanare pentru aplicație** nu sunt selectate reguli pentru zona de încredere, [aplicația de încredere este inclusă în scanare](#). În acest caz, aplicația de încredere nu este eliminată din lista de aplicații de încredere, însă caseta de selectare corespunzătoare este debifată.

e. În fereastra **Excluderi de la scanare pentru aplicație**, fă clic pe **OK**.

7. Pentru a elimina o aplicație din lista de aplicații de încredere:

a. Selectează o aplicație din lista de aplicații de încredere.

b. Fă clic pe butonul **Eliminare**.

8. În fereastra **Zonă de încredere**, fă clic pe **OK**.

9. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea și dezactivarea regulilor pentru zona de încredere pentru o aplicație din lista de aplicații de încredere

*Pentru a activa sau a dezactiva acțiunea aplicată de regulile pentru zona de încredere asupra unei aplicații din lista de aplicații de încredere:*

1. Deschide [fereastra cu setările aplicației](#).

2. Selectează secțiunea **Protecție antivirus** din stânga.

Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.

3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.

Se deschide fereastra **Zonă de încredere**.

4. În fereastra **Zonă de încredere**, selectează fila **Aplicații de încredere**.

5. În lista de aplicații de încredere, selectează aplicația de încredere respectivă.

6. Efectuează una dintre următoarele acțiuni:

- Pentru a exclude o aplicație de încredere de la scanarea Kaspersky Endpoint Security, bifează caseta de selectare de lângă numele ei.
- Pentru a include o aplicație de încredere în scanarea Kaspersky Endpoint Security, debifează caseta de selectare de lângă numele ei.

7. Fă clic pe **OK**.

8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Folosirea depozitului de certificate de sistem de încredere

Folosirea depozitului de certificate de sistem de încredere îți permite să excluzi de la scanările de viruși aplicațiile semnate cu o semnătură digitală de încredere. Kaspersky Endpoint Security atribuie automat astfel de aplicații grupului *De încredere*.

*Pentru a începe să folosești depozitul de certificate de sistem de încredere:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Protecție antivirus** din stânga.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Zonă de încredere**.
4. În fereastra **Zonă de încredere**, selectează fila **Depozit certificate de sistem de încredere**.
5. Bifează caseta de selectare **Utilizare depozit de certificate de sistem de încredere**.
6. În lista verticală **Depozit certificate de sistem de încredere**, selectează ce depozit de sistem al Kaspersky Endpoint Security trebuie să fie considerat de încredere.
7. În fereastra **Zonă de încredere**, fă clic pe **OK**.
8. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Autoprotecția aplicației Kaspersky Endpoint Security

Această secțiune prezintă mecanismele de autoprotecție și de protecție împotriva controlului la distanță ale aplicației Kaspersky Endpoint Security și oferă instrucțiuni privind configurarea setărilor acestor mecanisme.

## Despre Autoprotecția aplicației Kaspersky Endpoint Security

Kaspersky Endpoint Security protejează computerul de programe rău intenționate, inclusiv malware care încearcă să blocheze funcționarea Kaspersky Endpoint Security sau chiar să șteargă aplicația de pe computer.

Stabilitatea sistemului de securitate de pe computer este asigurată de mecanismele de autoprotecție și de apărare cu control la distanță din Kaspersky Endpoint Security.

Mecanismul de *Autoprotecție* previne alterarea sau ștergerea fișierelor aplicației de pe unitatea de hard disk, din procesele de memorie și din înregistrările din registrul de sistem.

*Protecția Control la distanță* blochează toate încercările de a controla serviciile aplicației de la un computer la distanță.

Pe computerele care execută sistemele de operare pe 64 de biți este disponibilă numai Autoprotecția Kaspersky Endpoint Security pentru prevenirea alterării și ștergerii fișierelor aplicației de pe unitatea de hard disk și a înregistrărilor de registru de sistem.

## Activarea sau dezactivarea Autoprotecției

Mecanismul de autoprotecție a aplicației Kaspersky Endpoint Security este activat în mod implicit. Dacă este necesar, poți dezactiva Autoprotecția.

*Pentru a activa sau a dezactiva Autoprotecția:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa mecanismul de autoprotecție, bifează caseta de selectare **Activare Autoprotecție**.
  - Pentru a dezactiva mecanismul de autoprotecție, debifează caseta de selectare **Activare Autoprotecție**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea sau dezactivarea protecției împotriva controlului la distanță

Mecanismul de protecție împotriva controlului la distanță este activat în mod implicit. Dacă este necesar, poți dezactiva mecanismul de protecție împotriva controlului la distanță.

*Pentru a activa sau a dezactiva mecanismul de protecție împotriva controlului la distanță:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Pentru a activa mecanismul de protecție împotriva controlului la distanță, bifează **Dezactivare gestionare externă a serviciului de sistem**.
  - Pentru a dezactiva mecanismul de protecție împotriva controlului la distanță, debifează **Dezactivare gestionare externă a serviciului de sistem**.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Acceptarea aplicațiilor de administrare la distanță

Ocazional, este posibil să ai nevoie să folosești o aplicație de administrare la distanță, în timp ce este activată protecția împotriva controlului extern.

*Pentru a activa funcționarea aplicațiilor de administrare la distanță:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Protecție antivirus** din stânga.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Excluderi de la scanare și aplicații de încredere**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Zonă de încredere**.
4. În fereastra **Zonă de încredere**, selectează fila **Aplicații de încredere**.
5. Fă clic pe butonul **Adăugare**.
6. În meniul contextual care se deschide, efectuează una dintre următoarele acțiuni:
  - Pentru a găsi aplicația de administrare la distanță în lista aplicațiilor instalate pe computer, selectează elementul **Aplicații**.  
Se deschide fereastra **Selectare aplicația**.

- Pentru a preciza calea către fișierul executabil al aplicației relevante, selectează **Răsfoire**.  
Se deschide fereastra Microsoft Windows standard **Deschidere fișier** (Deschidere fișier).

7. Selectează aplicația într-unul din modulele următoare:

- Dacă ai selectat **Aplicații** la pasul precedent, selectează aplicația în lista de aplicații instalate pe computer și fă clic pe **OK** în fereastra **Selectare aplicația**.
- Dacă ai selectat **Răsfoire** la pasul precedent, specifică o cale către fișierul executabil al aplicației relevante și fă clic pe butonul **Deschis** în fereastra standard **Deschis** din Microsoft Windows.

Aceste acțiuni determină deschiderea ferestrei **Excluderi de la scanare pentru aplicație**.

8. Bifează caseta de selectare **Nu monitoriza activitatea aplicației**.

9. În fereastra **Excluderi de la scanare pentru aplicație**, fă clic pe **OK**.

Aplicația de încredere pe care ai adăugat-o apare în lista de aplicații de încredere.

10. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Performanțele aplicației Kaspersky Endpoint Security și compatibilitatea acesteia cu alte aplicații

Această secțiune conține informații despre performanțele aplicației Kaspersky Endpoint Security și compatibilitatea acesteia cu alte aplicații, precum și indicații pentru selectarea tipurilor de obiecte detectabile și a modului de funcționare a aplicației Kaspersky Endpoint Security.

## Despre performanțele aplicației Kaspersky Endpoint Security și compatibilitatea acesteia cu alte aplicații

### Performanțele Kaspersky Endpoint Security

Performanțele Kaspersky Endpoint Security se referă la numărul de tipuri de obiecte ce-ți pot afecta computerul și care pot fi detectate, precum și la consumul de energie și utilizarea resurselor computerului.

### Selectarea tipurilor de obiecte detectabile

Kaspersky Endpoint Security îți permite să ajustezi protecția computerului și să selectezi [tipurile de obiecte](#) pe care le detectează aplicația în timpul funcționării. Kaspersky Endpoint Security scanează întotdeauna sistemul de operare după viruși, viermi și troieni. Nu poți dezactiva scanarea pentru aceste tipuri de obiecte. Aceste programe malware pot determina pagube grave computerului. Pentru o securitate mai mare pe computer, poți extinde gama de tipuri de obiecte detectabile activând monitorizarea software-ului legal care poate fi folosit de infractori pentru a-ți pune în pericol computerul sau datele personale.

## Folosirea modului de economisire a energiei

Consumul de energie de către aplicații este un factor cheie pentru computerele portabile. Activitățile planificate ale Kaspersky Endpoint Security de regulă folosesc resurse considerabile. Atunci când computerul rulează pe baterii, poți folosi modul economisire a energiei pentru a consuma mai puțină putere.

În modul de economisire a energiei, următoarele activități planificate sunt în mod automat amânate:

- [Activitate de actualizare](#)
- [Activitate de scanare completă](#)
- [Activitate de scanare a zonelor critice](#)
- [Activitate de scanare particularizată](#)
- [Activitate de scanare de vulnerabilități](#)
- [Activitate de verificare integritate](#)

În funcție de activarea sau nu a modului de economisire a energiei, Kaspersky Endpoint Security pune în pauză activitățile de criptare atunci când un computer portabil trece pe baterie. Aplicația reia activitățile de criptare atunci când computerul portabil trece de la alimentarea pe baterie pe cea de la priză.

## Cedarea de resurse pentru alte aplicații

Utilizarea resurselor computerului de către Kaspersky Endpoint Security poate afecta performanțele altor aplicații. Pentru a rezolva problema funcționării simultane în timp ce procesorul și subsistemele unității de hard disk sunt supuse unui flux de lucru sporit, Kaspersky Endpoint Security poate pune în pauză activitățile planificate și poate ceda resurse altor aplicații.

Cu toate acestea, o serie de aplicații pornesc imediat ce devin disponibile resurse de procesor, lucrând în fundal. Pentru ca scanarea să nu depindă de performanțele altor aplicații, este mai bine să nu li se cedeze resurse ale sistemului de operare.

Poți porni aceste activități manual, dacă este necesar.

## Utilizarea tehnologiei de dezinfectare avansată

Programele rău intenționate de azi pot pătrunde în zonele cele mai adânci ale sistemului de operare, ceea ce la face practic imposibil de eliminat. După detectarea unei activități rău intenționate în sistemul de operare, Kaspersky Endpoint Security execută o procedură de dezinfectare extinsă care folosește o [tehnologie de dezinfectare avansată](#). *Tehnologia de dezinfectare avansată* are rolul de a curăța sistemul de operare de programe rău intenționate care și-au început deja procesele în memoria RAM și care împiedică eliminarea lor de către Kaspersky Endpoint Security prin alte metode. Prin urmare, amenințarea este neutralizată. În timp ce dezinfectarea avansată este în curs, ți se recomandă să nu pornești procese noi și să nu editezi registrul sistemului de operare. Tehnologia de dezinfectare avansată folosește resurse ale sistemului de operare considerabile, care pot încetini alte aplicații.

După finalizarea procesului de dezinfectare avansată pe un computer pe care se execută Microsoft Windows pentru stații de lucru, Kaspersky Endpoint Security solicită utilizatorului permisiunea de a reporni computerul. După repornirea sistemului, Kaspersky Endpoint Security șterge fișierele programului malware și pornește o scanare completă a computerului.

O solicitare de repornire este imposibilă pe un computer care execută Microsoft Windows pentru servere de fișiere, din cauza aspectelor specifice ale activității aplicației Kaspersky Endpoint Security pentru servere de fișiere. O repornire neplanificată a unui server de fișiere poate conduce la probleme implicând indisponibilitatea temporară a datelor din serverul de fișiere sau pierderea unor date nesalvate. Se recomandă repornirea unui server de fișiere strict conform planificării. De aceea dezinfectarea avansată este [dezactivată](#) în mod implicit pentru serverele de fișiere.

Dacă pe un server de fișiere este detectată o infecție activă, este transmis un eveniment către Kaspersky Security Center cu informația că este necesară dezinfectarea avansată. Pentru dezinfectarea unei infecții active de pe un server de fișiere, activează tehnologia de dezinfectare activă pentru servere de fișiere și pornește o activitate de grup *Scanare viruși* într-un moment convenabil pentru utilizatorii serverului de fișiere.

## Selectarea tipurilor de obiecte detectabile

*Pentru a selecta tipurile de obiecte detectabile:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Protecție antivirus**.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În secțiunea **Obiecte**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Obiecte pentru detectare**.



4. Bifează casetele de selectare de lângă obiectele pe care dorești să le detecteze Kaspersky Endpoint Security:

- **instrumente periculoase**
- **Adware**
- **Programe de apelare automată**
- **Altele**
- **Fișiere împachetate care pot fi dăunătoare**
- **Fișiere împachetate multiplu**

5. Fă clic pe **OK**.

Se închide fereastra **Obiecte pentru detectare**. În secțiunea **Obiecte**, tipurile de obiecte selectate sunt listate sub **Detecția următoarelor tipuri de obiecte este activată**.

6. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea sau dezactivarea tehnologiei de dezinfectare avansată pentru stații de lucru

*Pentru a activa sau a dezactiva tehnologia de dezinfectare avansată pentru stații de lucru:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Protecție antivirus**.  
Setările protecției antivirus sunt afișate în partea dreaptă a ferestrei.
3. În partea dreaptă a ferestrei, efectuează una dintre următoarele acțiuni:
  - Selectează **Activare tehnologie dezinfectare avansată** pentru a activa tehnologia de dezinfectare avansată.
  - Debifează **Activare tehnologie dezinfectare avansată** pentru a dezactiva tehnologia de dezinfectare avansată.
4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

Atunci când activitatea Dezinfecare avansată este lansată prin Kaspersky Security Center, majoritatea funcțiilor sistemului de operare nu sunt disponibile utilizatorului. Stația de lucru va fi repornită după finalizarea activității.

## Activarea sau dezactivarea tehnologiei de dezinfecare avansată pentru servere de fișiere

*Pentru a activa tehnologia de dezinfecare avansată pentru servere de fișiere, efectuează una din următoarele acțiuni:*

- Activează tehnologia de dezinfecare avansată din proprietățile politicii Kaspersky Security Center active. Pentru aceasta:
  - a. Deschide secțiunea **Setări de protecție generale** în fereastra de proprietăți a politicii.
  - b. Bifează caseta de selectare **Activare tehnologie dezinfecare avansată**.
  - c. Pentru a salva modificările, fă clic pe **OK** în fereastra de proprietăți a politicii.
- În fereastra de proprietăți a activității de grup Scanare de viruși din Kaspersky Security Center, bifează caseta de selectare **Execută Dezinfecare avansată imediat**.

*Pentru a dezactiva tehnologia de dezinfecare avansată pentru servere de fișiere, efectuează una din următoarele acțiuni:*

- Activează tehnologia de dezinfecare avansată din proprietățile politicii Kaspersky Security Center. Pentru aceasta:
  - a. Deschide secțiunea **Setări de protecție generale** în fereastra de proprietăți a politicii.
  - b. Debifează caseta de selectare **Activare tehnologie dezinfecare avansată**.
  - c. Pentru a salva modificările, fă clic pe **OK** în fereastra de proprietăți a politicii.
- În fereastra de proprietăți a activității de grup Scanare de viruși din Kaspersky Security Center, debifează caseta de selectare **Execută Dezinfecare avansată imediat**.

## Activarea sau dezactivarea modului de economisire a energiei

*Pentru a activa sau a dezactiva modul de conservare a energiei:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.

Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.

3. În secțiunea **Mod de funcționare**, fă clic pe butonul **Setări**.

Se deschide fereastra **Mod de funcționare**.

4. Efectuează următoarele acțiuni în secțiunea **Mod de funcționare**:

- Pentru a activa modul de conservare a energiei, bifează caseta de selectare **Amână activități planificate la funcționarea cu alimentare de la baterie**.

Atunci când modul de conservare a energiei este activat și computerul funcționează cu alimentare de la baterie, următoarele activități nu sunt executate, chiar dacă sunt planificate:

- Activitate de actualizare
  - Activitate de scanare completă
  - Activitate de scanare a zonelor critice
  - Activitate de scanare particularizată
  - Activitate de scanare de vulnerabilități
  - Activitate de verificare integritate
- Dacă dorești să dezactivezi modul de conservare a energiei, debifează caseta de selectare **Amână activități planificate la funcționarea cu alimentare de la baterie**. În acest caz, Kaspersky Endpoint Security execută activitățile planificate, indiferent de sursa de alimentare a computerului.

5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Activarea sau dezactivarea cedării de resurse pentru alte aplicații

*Pentru a activa sau a dezactiva cedarea de resurse pentru alte aplicații:*

1. Deschide [fereastra cu setările aplicației](#).

2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.

Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.

3. În secțiunea **Mod de funcționare**, fă clic pe butonul **Setări**.

Se deschide fereastra **Mod de funcționare**.

#### 4. Efectuează următoarele acțiuni în secțiunea **Mod de funcționare**:

- Dacă dorești să activezi modul în care sunt cedate resurse altor aplicații, bifează caseta de selectare **Cedare resurse pentru alte aplicații**.

Atunci când este configurat să cedeze resurse altor aplicații, Kaspersky Endpoint Security amână activitățile planificate care încetinesc alte aplicații:

- Activitate de actualizare
  - Activitate de scanare completă
  - Activitate de scanare a zonelor critice
  - Activitate de scanare particularizată
  - Activitate de scanare de vulnerabilități
  - Activitate de verificare integritate
- Dacă dorești să dezactivezi modul în care sunt cedate resurse altor aplicații, debifează caseta de selectare **Cedare resurse pentru alte aplicații**. În acest caz, Kaspersky Endpoint Security execută activitățile planificate, indiferent de funcționarea altor aplicații.

În mod implicit, aplicația este configurată să cedeze resurse pentru alte aplicații.

#### 5. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Protecția prin parolă

Această secțiune conține informații privind restricționarea accesului la aplicația Kaspersky Endpoint Security cu ajutorul unei parole.

## Despre restricționarea accesului la Kaspersky Endpoint Security

Pe un computer pot avea acces mai mulți utilizatori, cu niveluri diferite de cunoștințe privind computerele. Dacă utilizatorii ar avea acces nelimitat la Kaspersky Endpoint Security și la setările sale, nivelul general de protecție a computerului s-ar putea reduce.

Poți restricționa accesul la Kaspersky Endpoint Security setând un nume de utilizator și o parolă și specificând operațiunile pentru care aplicația solicită utilizatorului aceste drepturi:

Atunci când se face upgrade pentru o versiune anterioară a aplicației la Kaspersky Endpoint Security 10 Service Pack 2 for Windows, parola se păstrează (dacă a fost setată). Pentru a edita pentru prima dată setările de protecție prin parolă, folosește numele de utilizator implicit KLAdmin.

## Activarea și dezactivarea protecției prin parolă

Recomandăm atenție atunci când utilizezi o parolă pentru a restricționa accesul la aplicație. Dacă ai uitat parola, [contactează asistența tehnică de la Kaspersky](#) pentru instrucțiuni despre dezactivarea protecției prin parolă.

*Pentru a activa protecția prin parolă:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările aplicației sunt afișate în dreapta ferestrei.
3. În secțiunea **Protecție prin parolă**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Protecție prin parolă**.
4. Bifează caseta de selectare **Activare protecție prin parolă**.
5. În câmpul **Nume utilizator**, introdu numele de utilizator care trebuie specificat în fereastra **Verificare parolă** la efectuarea ulterioară a operațiunilor protejate prin parolă.
6. În câmpul **Parolă nouă**, tastează o parolă pentru accesarea aplicației.
7. Confirmă parola în câmpul **Confirmare parolă**.
8. Dacă dorești să restricționezi accesul pentru toate operațiunile aplicației, în secțiunea **Domeniu parolă**, fă clic pe butonul **Selectare totală**.
9. Dacă dorești să restricționezi selectiv accesul utilizatorului, în secțiunea **Domeniu parolă**, bifează casetele de selectare de lângă numele operațiunilor relevante:
  - **Configurare setări aplicație.**
  - **Ieșire din aplicație.**
  - **Dezactivează componentele protecției.**

- **Dezactivare componente de control.**
- **Eliminare cheie.**
- **Eliminare/modificare/restaurare aplicație.**
- **Restabilire acces la date de pe unități criptate.**
- **Vizualizare rapoarte.**

10. Fă clic pe butonul **OK**.

Aplicația verifică parolele introduse. Dacă parolele se potrivesc, aplicația aplică parola. Dacă parolele nu se potrivesc, aplicația îți solicită să confirmi din nou parola în câmpul **Confirmare parolă**.

După activarea protecției prin parolă, aplicația va solicita o parolă de fiecare dată când se efectuează o operațiune inclusă în domeniul parolei. Dacă nu dorești ca aplicația să-ți solicite parola de fiecare dată când încerci să efectuezi o operațiune protejată prin parolă în sesiunea curentă, poți bifa caseta de selectare **Salvare parolă pentru sesiunea curentă** în fereastra **Verificare parolă**.

Atunci când caseta de selectare **Salvare parolă pentru sesiunea curentă** nu este bifată, aplicația îți va solicita parola de fiecare dată când încerci să efectuezi operațiunea protejată prin parolă.

*Pentru a dezactiva protecția prin parolă:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările aplicației sunt afișate în dreapta ferestrei.
3. În secțiunea **Protecție prin parolă**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Protecție prin parolă**.
4. Debifează caseta de selectare **Activare protecție prin parolă**.

Puteți dezactiva protecția prin parolă numai dacă sunteți autentificat ca KLAdmin. Nu este posibil să dezactivați protecția prin parolă dacă utilizați un alt cont de utilizator sau o parolă temporară.

5. Fă clic pe butonul **OK**.

După dezactivarea protecției prin parolă, accesul restricționat la aplicație va fi anulat la următoarea pornire a aplicației Kaspersky Endpoint Security.

## Modificarea parolei de acces la Kaspersky Endpoint Security

*Pentru a modifica parola de acces pentru Kaspersky Endpoint Security:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.
3. În secțiunea **Protecție prin parolă**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Protecție prin parolă**.
4. Introdu numele de utilizator în câmpul **Nume utilizator**.
5. În câmpul **Parolă nouă**, introdu o parolă nouă pentru accesul la aplicație.
6. În câmpul **Confirmare parolă**, introdu din nou noua parolă.
7. Fă clic pe **OK**.  
Aplicația verifică parolele introduse. Dacă parolele se potrivesc, aplicația aplică parola nouă și închide fereastra **Protecție prin parolă**. Dacă parolele nu se potrivesc, aplicația îți solicită să confirmi din nou parola în câmpul **Confirmare parolă**.
8. Pentru a salva modificările, în fereastra de setări ale aplicației, fă clic pe butonul **Salvare**.

## Despre folosirea unei parole temporare

Atunci când lucrezi pe computere client gestionate de o politică a Kaspersky Security Center, este posibil ca utilizatorii să trebuiască să efectueze operațiuni cu aplicația Kaspersky Endpoint Security care sunt protejate prin parolă la nivel de politică. Atunci când protecția prin parolă este activată, doar administratorul Kaspersky Security Center poate efectua operațiunile specificate în domeniul parolei. Cu toate acestea, dacă se pierde conexiunea cu aplicația Kaspersky Security Center (de exemplu, atunci când utilizatorul este în afara rețelei companiei), funcțiile disponibile pentru lucrul cu interfața locală a Kaspersky Security Center sunt limitate.

Pentru a furniza unui utilizator capacitatea de efectua operațiunile necesare fără a-i oferi parola setată în setările politicii, administratorul Kaspersky Security Center poate crea o parolă temporară. O parolă temporară are o perioadă de valabilitate limitată și un domeniu de acțiune limitat. După ce utilizatorul introduce parola temporară în interfața locală a aplicației, devin disponibile operațiunile permise de către administratorul Kaspersky Security Center.

Atunci când parola temporară expiră, Kaspersky Endpoint Security continuă să funcționeze conform setărilor din politica aplicației Kaspersky Security Center. Operațiunile care sunt protejate prin parolă la nivel de politică nu mai sunt disponibile pentru utilizator.

## Crearea unei parole temporare folosind Consola de administrare Kaspersky Security Center

*Pentru a crea o parolă temporară și a o trimite unui utilizator:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul utilizatorului care solicită parola temporară.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. În meniul contextual al computerului care aparține utilizatorului de solicită parola temporară, selectează **Proprietăți**.

Se deschide fereastra **Proprietăți: <Nume computer>**.

5. În fereastra **Proprietăți: <Nume computer>**, selectează secțiunea **Aplicații**.
6. Selectează Kaspersky Endpoint Security Service Pack 2 for Windows și deschide fereastra de proprietăți a aplicației folosind una dintre următoarele metode:

- Fă clic pe butonul **Proprietăți** în partea de jos a ecranului.
- În meniul contextual al aplicației, selectează **Proprietăți**.

Această acțiune deschide fereastra **Setări aplicație „<Nume aplicație>”**.

7. În fereastra **Setări aplicație „<Nume aplicație>”**, în secțiunea **Setări avansate**, selectează subsecțiunea **Setări aplicație**.

8. În secțiunea **Protecție prin parolă**, fă clic pe butonul **Setări**.

Se deschide fereastra **Protecție prin parolă**.

9. În fereastra **Protecție prin parolă**, în secțiunea **Parolă temporară**, fă clic pe butonul **Setări**.

Acest buton este disponibil dacă protecția prin parolă este activată pentru Kaspersky Security Center în politica aplicației Kaspersky Security Center care se execută pe computer.



Se deschide fereastra **Creare parolă temporară**.

10. În câmpul **Dată expirare**, specifică data la care utilizatorul nu va mai putea să folosească parola temporară.

La acea dată parola temporară devine nevalidă. Trebuie creată o parolă temporară nouă pentru a furniza acces la operațiunile din interfața locală a Kaspersky Endpoint Security.

11. În tabelul **Domeniu parolă temporară**, bifează casetele de selectare de lângă operațiunile care trebuie să fie disponibile pentru utilizator atunci când este valabilă parola temporară.

12. Fă clic pe butonul **Creare**.

Această acțiune deschide fereastra **Parolă temporară**, care conține o parolă criptată.

13. Copiază parola și [instrucțiunile privind aplicarea parolei](#) și trimite-le utilizatorului.

## Aplicarea unei parole temporare în interfața Kaspersky Endpoint Security

Aceste instrucțiuni sunt destinate utilizatorilor computerelor client pe care este instalat Kaspersky Endpoint Security.

*Pentru a aplica o parolă temporară:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările aplicației sunt afișate în dreapta ferestrei.
3. În secțiunea **Protecție prin parolă**, fă clic pe butonul **Parolă temporară**.  
Se deschide fereastra **Parolă temporară**.
4. Bifează caseta de selectare **Activare parolă temporară**.
5. În câmpul de introducere, specifică parola obținută de la administratorul Kaspersky Security Center.
6. Fă clic pe **OK** pentru a salva modificările.

După aplicarea parolei temporare, operațiunile specificate de administratorul Kaspersky Security Center devin disponibile. Fereastra **Parolă temporară** afișează data expirării parolei temporare și operațiunile permise.

# Administrarea la distanță a aplicației prin Kaspersky Security Center

Această secțiune prezintă administrarea aplicației Kaspersky Endpoint Security prin aplicația Kaspersky Security Center.

## Despre gestionarea aplicației prin Kaspersky Security Center

De la distanță, Kaspersky Security Center îți permite să instalezi și să deinstalezi, să pornești și să oprești Kaspersky Endpoint Security, să configurezi setările aplicației, să modifice setul de componente ale aplicației disponibile, să adaugi chei și să pornești activități de actualizare și scanare.

Pentru informații suplimentare despre gestionarea aplicației prin Kaspersky Security Center, informații care nu sunt furnizate în acest document, consultă *Ghidul administratorului Kaspersky Security Center*.

Aplicația poate fi gestionată prin Kaspersky Security Center folosind plug-inul de administrare Kaspersky Endpoint Security.

Versiunea plug-inului de administrare poate fi diferită de versiunea de Kaspersky Endpoint Security instalată pe computerul client. Dacă versiunea de plug-in de administrare instalată are mai puține funcționalități decât versiunea de Kaspersky Endpoint Security, setările pentru funcțiile care lipsesc nu vor fi reglementate prin plug-inul de administrare. Aceste setări pot fi modificate de către utilizator în interfața locală a Kaspersky Endpoint Security.

## Considerații speciale pentru lucru cu versiuni diferite ale plug-inurilor de administrare

Poți folosi un plug-in de administrare pentru a modifica următoarele elemente:

- Politici
- Profiluri de politici
- Activități de grup
- Activități locale
- Setări locale ale Kaspersky Endpoint Security

Poți gestiona Kaspersky Endpoint Security prin intermediul Kaspersky Security Center numai dacă ai un plug-in de administrare cu versiune egală sau mai mare decât versiunea specificată în informațiile privind compatibilitatea aplicației Kaspersky Endpoint Security cu plug-inul de administrare. Poți vizualiza versiunea minimă necesară a plug-inului de administrare în fișierul installer.ini inclus în [kitul de distribuire](#).

Dacă este deschisă orice componentă, plug-inul de administrare verifică informațiile de compatibilitate. Dacă versiunea plug-inului de administrare este egală sau ulterioară versiunii specificate în informațiile de compatibilitate, poți modifica setările acestei componente. În caz contrar, nu poți folosi plug-inul de administrare pentru a modifica setările componente selectate. Se recomandă upgrade-ul plug-inului de administrare.

## Modificarea setărilor definite anterior folosind o versiune ulterioară a plug-inului de administrare

Poți folosi o versiune ulterioară a plug-inului de administrare pentru a modifica toate setările definite anterior și poți configura setări noi care nu erau prezente în versiunea de plug-in de administrare folosită anterior.

Pentru setările noi, o versiune ulterioară a plug-inului de administrare atribuie valori implicite atunci când o politică, un profil de politică sau o activitate este salvat(ă) pentru prima dată.

După ce modifizi o politică, un profil de politică sau o activitate de grup folosind o versiune ulterioară a plug-inului de administrare, aceste componente nu vor mai fi disponibile pentru versiuni anterioare ale plug-inului de administrare. Setările locale ale aplicației Kaspersky Endpoint Security și setările activităților locale vor fi în continuare disponibile pentru plug-inul de administrare al versiunilor anterioare.

## Pornirea și oprirea Kaspersky Endpoint Security pe un computer client

*Pentru a porni și a opri aplicația pe un computer client:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele [grupului de administrare](#) ? căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. Selectează computerul pe care dorești să pornești sau să oprești aplicația.
5. Fă clic dreapta pentru a afișa meniul contextual al computerului client și selectează **Proprietăți**.  
Se deschide fereastra de proprietăți a computerului client.

6. În fereastra de proprietăți a computerului client, selectează secțiunea **Aplicații**.

În dreapta ferestrei Proprietăți computer client apare o listă de aplicații Kaspersky instalate pe computerul client.

7. Selectează Kaspersky Endpoint Security 10 for Windows.

8. Efectuează următoarele acțiuni:

- Pentru a porni aplicația, faceți clic pe butonul  din dreapta listei de aplicații Kaspersky sau procedează astfel:

a. Selectează **Proprietăți** în meniul contextual al Kaspersky Endpoint Security sau fă clic pe butonul **Proprietăți** amplasat sub lista de aplicații Kaspersky.

Apare fereastra **de setări pentru aplicația Kaspersky Endpoint Security 10 for Windows**.

b. În secțiunea **General**, fă clic pe butonul **Executare** în partea dreaptă a ferestrei.

- Pentru a opri aplicația, fă clic pe butonul  din dreapta listei de aplicații Kaspersky sau procedează astfel:

a. Selectează **Proprietăți** în meniul contextual al Kaspersky Endpoint Security sau fă clic pe butonul **Proprietăți** amplasat sub lista de aplicații Kaspersky.

Apare fereastra **de setări pentru aplicația Kaspersky Endpoint Security 10 for Windows**.

b. În secțiunea **General**, fă clic pe butonul **Opre** în partea dreaptă a ferestrei.

## Configurarea setărilor Kaspersky Endpoint Security

*Pentru a configura setările Kaspersky Endpoint Security:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare ? căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. Selectează computerul pentru care dorești să configurezi setările Kaspersky Endpoint Security.
5. În meniul contextual al computerului client, selectează **Proprietăți**.  
Se deschide fereastra de proprietăți a computerului client.
6. În fereastra de proprietăți a computerului client, selectează secțiunea **Aplicații**.

În dreapta ferestrei **Proprietăți** computer client apare o listă de aplicații Kaspersky instalate pe computerul client.

7. Selectează aplicația Kaspersky Endpoint Security 10 pentru Windows.

8. Efectuează una dintre următoarele acțiuni:

- Selectează **Proprietăți** din meniul contextual al Kaspersky Endpoint Security 10 for Windows.
- Fă clic pe butonul **Proprietăți** de sub lista de aplicații Kaspersky.

Apare fereastra **de setări pentru aplicația Kaspersky Endpoint Security 10 for Windows**.

9. În secțiunea **Setări avansate**, configurează setările pentru Kaspersky Endpoint Security, precum și setările pentru rapoarte și stocare.

Celelalte secțiuni din fereastra de **setări pentru aplicația Kaspersky Endpoint Security 10 for Windows** sunt identice cu cele din secțiunile pentru aplicația standard Kaspersky Security Center. O descriere a acestor secțiuni este furnizată în *Ghidul administratorului Kaspersky Security Center*.

Dacă o aplicație este subiectul unei politici care interzice modificările unor setări specifice, nu vei putea să le editezi atunci când configurezi setările aplicației în secțiunea **Setări avansate**.

10. Pentru a salva modificările, în fereastra **Setări pentru aplicația Kaspersky Endpoint Security 10 for Windows**, fă clic pe **OK**.

## Gestionarea activităților

Această secțiune descrie cum se gestionează activitățile Kaspersky Endpoint Security. Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii despre gestionarea activităților în Kaspersky Security Center.

## Despre activitățile pentru Kaspersky Endpoint Security

Kaspersky Security Center controlează activitatea aplicațiilor Kaspersky pe computerele client prin intermediul activităților. Activitățile implementează funcții administrative principale, cum ar fi instalarea cheii, scanarea computerului și actualizări ale bazei de date și ale modulelor software ale aplicației.

Poți crea următoarele tipuri de activități pentru a administra Kaspersky Endpoint Security folosind Kaspersky Security Center:

- Activități locale care sunt configurate pentru un computer client individual.
- Activități de grup care sunt configurate pentru computere client din grupuri de administrare.
- Activități pentru un set de computere care nu aparțin unor grupuri de administrare.

Activitățile pentru seturi de computere din afara grupurilor de administrare se aplică numai computerelor client specificate în setările activității. Dacă noi computere client sunt adăugate la un set de computere pentru care este configurată o activitate, această activitate nu se aplică acestor noi computere. Pentru a aplica activitatea acestor computere, creează o activitate nouă sau editează setările activității existente.

Pentru a administra de la distanță Kaspersky Endpoint Security, poți folosi următoarele activități cu oricare dintre tipurile menționate:

- **Adăugare cheie.** Kaspersky Endpoint Security adaugă o cheie pentru activarea aplicației, inclusiv o cheie suplimentară.
- **Modificare componente ale aplicației.** Kaspersky Endpoint Security instalează sau elimină componente pe computere client, în conformitate cu lista de componente din setările activității.
- **Inventar.** Kaspersky Endpoint Security colectează informații despre toate fișierele executabile ale aplicațiilor care sunt stocate pe computere.

Poți activa inventarul pentru module DLL și fișiere script. În acest caz, Kaspersky Security Center va primi informații despre modulele DLL încărcate pe un computer pe care este instalat Kaspersky Endpoint Security și despre fișierele care conțin scripturi.

Activarea inventarului pentru module DLL și fișiere script mărește semnificativ durata activității de inventar și mărimea bazei de date.

- **Actualizare.** Kaspersky Endpoint Security actualizează bazele de date și modulele aplicației conform setărilor de actualizare configurate.
- **Restaurare.** Kaspersky Endpoint Security derulează înapoi ultima actualizare a bazelor de date și a modulelor.
- **Scanare viruși.** Kaspersky Endpoint Security scanează de viruși și alte amenințări zonele din computer specificate în setările activității.
- **Verificare conexiune la KSN.** Kaspersky Endpoint Security trimite o solicitare despre disponibilitatea serverelor KSN și actualizează starea conexiunii KSN.

- **Verificare integritate.** Kaspersky Endpoint Security primește date despre setul de module de aplicație instalate pe computerul client și scanează semnătura digitală pentru fiecare modul.
- **Gestionare conturi Agent de Autentificare.** Atunci când efectuează această activitate, Kaspersky Endpoint Security generează comenzi pentru eliminarea, adăugarea sau modificarea conturilor de Agent de Autentificare.

Poți efectua următoarele acțiuni cu activitățile:

- Pornire, oprire, suspendare și reluare activități.
- Creare activități noi.
- Editare setări activitate.

Drepturile de accesare a setărilor activităților Kaspersky Endpoint Security (citire, scriere, executare) sunt definite pentru fiecare utilizator care are acces la serverul de administrare Kaspersky Security Center, prin setările de acces la zonele operaționale ale Kaspersky Endpoint Security. Pentru a configura accesul la zonele operaționale ale Kaspersky Endpoint Security, accesează secțiunea **Securitate** din fereastra de proprietăți a serverului de administrare Kaspersky Security Center.

## Configurarea modului de gestionare a activităților

*Pentru a configura modul în care se lucrează cu activitățile în interfața locală a Kaspersky Endpoint Security:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să configurezi lucrul cu activitățile în interfața locală a Kaspersky Endpoint Security.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În secțiunea **Setări avansate**, selectează subsecțiunea **Setări aplicație**.
7. În secțiunea **Mod de funcționare**:

- Dacă dorești să permiți utilizatorilor să lucreze cu activități locale în interfața și linia de comandă a Kaspersky Endpoint Security, bifează caseta de selectare **Permite utilizarea activităților locale**.

Dacă această casetă de selectare nu este bifată, funcțiile activităților locale sunt oprite. În acest mod, activitățile locale nu se execută conform planificării. Activitățile locale nu pot fi pornite și nici configurate în interfața locală a Kaspersky Endpoint Security sau atunci când se lucrează în linia de comandă.

- Dacă dorești să permiți utilizatorilor să vadă lista de activități de grup, bifează caseta de selectare **Permite afișarea activităților de grup**.
- Dacă dorești să permiți utilizatorilor să modifice setările activităților de grup, bifează caseta de selectare **Permite gestionare activități de grup**.

8. Fă clic pe **OK** pentru a salva modificările.

9. Aplică politica.

Consultă *Ghidul administratorului Kaspersky Security Center* pentru detalii referitoare la aplicarea politicii Kaspersky Security Center.

## Crearea unei activități locale

*Pentru a crea o activitate locală:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare ? căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. Selectează computerul pentru care dorești să creezi o activitate locală.
5. Efectuează una dintre următoarele acțiuni:
  - În meniul contextul al computerului client, selectează opțiunea **Toate activitățile** Creare activitate.
  - În meniul contextul al computerului client, selectează **Proprietăți** și, în fereastra **Proprietăți: <Nume computer>** care apare, în fila **Activități**, fă clic pe butonul **Adăugare**.
  - În lista verticală **Efectuare acțiune**, selectează **Creare activitate**.



Expertul de activitate pornește.

6. Urmează instrucțiunile din Expertul de activitate.

## Crearea unei activități de grup

*Pentru a crea o activitate de grup:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. Efectuează una dintre următoarele acțiuni:
  - Selectează directorul **Dispozitive administrate** al arborelui consolei de administrare pentru a crea o activitate de grup pentru toate computerele gestionate de Kaspersky Security Center.
  - În directorul **Dispozitive administrate** al arborelui consolei de administrare, selectează directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. Selectează fila **Activități** în spațiul de lucru.
4. Fă clic pe butonul **Creează o activitate**.  
Expertul de activitate pornește.
5. Urmează instrucțiunile din Expertul de activitate.

## Crearea unei activități pentru o selecție de dispozitive

*Pentru a crea o activitate pentru selectarea de dispozitive, efectuează următoarele acțiuni:*



1. Deschide consola de administrare a Kaspersky Security Center.
2. Selectează directorul **Activități** în arborele Consolei de administrare.
3. Fă clic pe butonul **Creează o activitate**.  
Expertul de activitate pornește.
4. Urmează instrucțiunile din Expertul de activitate.
5. În fereastra **Selectare dispozitive pentru care se va aplica activitatea** a Expertului, fă clic pe butonul **Aplicare activitate unei selecții de dispozitive**.
6. În următoarea fereastră a Expertului, fă clic pe butonul **Selectare**.  
Se deschide fereastra **Selecție de dispozitive**.

7. Selectează dispozitivele necesare.
8. Fă clic pe **OK** în fereastra **Seleție de dispozitive**.
9. Urmează instrucțiunile din Expertul de activitate.

## Pornirea, oprirea, suspendarea și reluarea unei activități

Dacă [aplicația Kaspersky Endpoint Security se execută](#) pe un computer client, poți porni, opri, suspenda și relua o activitate pe acest computer client folosind Kaspersky Security Center. Atunci când Kaspersky Endpoint Security este suspendat, activitățile în execuție sunt suspendate și este imposibil să pornești, să oprești, să suspenzi sau să reiei o activitate prin Kaspersky Security Center.

*Pentru a porni, a opri, a suspenda sau a relua o activitate locală:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele [grupului de administrare ?](#) căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. Selectează computerul pe care dorești să pornești, să oprești, să suspenzi sau să reiei o activitate locală.
5. Fă clic dreapta pentru a afișa meniul contextual al computerului client și selectează **Proprietăți**.  
Se deschide fereastra de proprietăți a computerului client.
6. Selectează secțiunea **Activități**.  
În dreapta ferestrei apare o listă de activități locale.
7. Selectează o activitate locală pe care dorești să o pornești, să o oprești, să o suspenzi sau să o reiei.
8. Efectuează acțiunea necesară asupra activității folosind una dintre metodele următoare:
  - Fă clic dreapta pentru a deschide meniul contextual al activității locale și selectează **Executare / Oprire / Pauză / Reluare**.
  - Pentru a porni sau a opri o activitate locală, fă clic pe butonul  /  din dreapta listei de activități locale.



- Efectuează următoarele acțiuni:
  - a. Fă clic pe butonul **Proprietăți** sub lista de activități locale sau selectează **Proprietăți** în meniul contextual al activității.

Se deschide fereastra **Proprietăți: <Nume activitate>**.

- b. În fila **General**, fă clic pe butonul **Executare / Opreire / Pauză / Reluare**.

*Pentru a porni, a opri, a pune în pauză sau a relua o activitate de grup:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare pentru care dorești să pornești, să oprești, să pui în pauză sau să reiei o activitate de grup.
3. Selectează fila **Activități** în spațiul de lucru.

Activitățile de grup sunt afișate în partea dreaptă a ferestrei.
4. Selectează o activitate de grup pe care dorești să o pornești, să o oprești, să o pui în pauză sau să o reiei.
5. Efectuează acțiunea necesară asupra activității folosind una dintre metodele următoare:
  - În meniul contextual al activității de grup, selectează **Executare / Opreire / Pauză / Reluare**.
  - Pentru a porni sau a opri o activitate de grup, fă clic pe butonul  /  din dreapta ferestrei.
  - Efectuează următoarele acțiuni:



- a. Fă clic pe linkul **Setări activități** în partea dreaptă a spațiului de lucru Consolă de administrare sau selectează **Proprietăți** în meniul contextual al activității.

Se deschide fereastra **Proprietăți: <Nume activitate>**.

- b. În fila **General**, fă clic pe butonul **Executare / Opreire / Pauză / Reluare**.

*Pentru a porni, a opri, a pune în pauză sau a relua o activitate pentru o selecție de computere:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Activități** din arborele consolei de administrare, selectează activitatea pentru o selecție de computere pe care dorești să o pornești, să o oprești, să o pui în pauză sau să o reiei.
3. Efectuează una dintre următoarele acțiuni:

- În meniul contextual al activității, selectează **Executare / Opreire / Pauză / Reluare**.
- Pentru a porni sau a opri activitatea pentru anumite computere, fă clic pe butonul  /  din dreapta ferestrei.
- Efectuează următoarele acțiuni:
  - a. Fă clic pe linkul **Setări activități** în partea dreaptă a spațiului de lucru Consolă de administrare sau selectează **Proprietăți** în meniul contextual al activității.  
Se deschide fereastra **Proprietăți: <Nume activitate>**.
  - b. În fila **General**, fă clic pe butonul **Executare / Opreire / Pauză / Reluare**.

## Editarea setărilor unei activități

*Pentru a edita setările pentru o activitate locală:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare ? căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectează fila **Dispozitive**.
4. Selectează un computer pentru care dorești să configurezi setările aplicației.
5. Fă clic dreapta pentru a afișa meniul contextual al computerului client și selectează **Proprietăți**.  
Se deschide fereastra de proprietăți a computerului client.
6. Selectează secțiunea **Activități**.  
În dreapta ferestrei apare o listă de activități locale.
7. Selectează activitatea locală respectivă în lista de activități locale.
8. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
9. În fereastra **Proprietăți: <Nume activitate locală>**, selectează secțiunea **Setări**.
10. Editează setările activității locale.

11. Pentru a salva modificările, în fereastra **Proprietăți: <Nume activitate locală>**, fă clic pe **OK**.

12. Pentru a salva modificările, în fereastra **Proprietăți: <Nume computer>**, fă clic pe **OK**.

*Pentru a edita setările pentru o activitate de grup:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate**, deschide directorul cu numele grupului de administrare relevant.
3. Selectează fila **Activități** în spațiul de lucru.  
Activitățile de grup sunt afișate în spațiul de lucru Consolă de administrare.
4. Selectează activitatea de grup necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
6. În fereastra **Proprietăți: <Nume activitate de grup>**, selectează secțiunea **Setări**.
7. Editează setările activității de grup.
8. Pentru a salva modificările, în fereastra **Proprietăți: <Nume activitate de grup>**, fă clic pe **OK**.

*Pentru a edita setările unei activități pentru o selecție de computere:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Activități** din arborele consolei de administrare, selectează activitatea pentru selecția de computere ale cărei setări dorești să le editezi.
3. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:
  - În meniul contextual al politicii, selectează **Proprietăți**.
  - Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.
4. În fereastra **Proprietăți: <Nume activitate pentru selecția de computere>**, selectează secțiunea **Setări**.

5. Editează setările activității pentru selecția de computere.
6. Pentru a salva modificările, în fereastra **Proprietăți: <Nume activitate pentru selecția de computere>**, fă clic pe **OK**.

Cu excepția secțiunii **Setări**, toate secțiunile din fereastra de proprietăți ale activității sunt identice cu cele folosite în Kaspersky Security Center. Pentru o descriere detaliată a acestora, consultați *Ghidul administratorului Kaspersky Security Center*. Secțiunea **Setări** conține setări specifice pentru Kaspersky Endpoint Security 10 for Windows. Conținutul său depinde de activitatea selectată sau de tipul activității.

## Gestionarea politicilor



Această secțiune descrie crearea și configurarea politicilor pentru Kaspersky Endpoint Security. Pentru informații mai detaliate despre gestionarea Kaspersky Endpoint Security folosind politicile Kaspersky Security Center, consultă *Ghidul administratorului Kaspersky Security Center*.

## Despre politici

Poți folosi politici pentru a aplica setări identice ale Kaspersky Endpoint Security pentru toate computerele client dintr-un grup de administrare.

Poți modifica la nivel local valorile setărilor specificate de o politică pentru computere individuale dintr-un grup de administrare folosind Kaspersky Endpoint Security. Poți modifica locale acele setări a căror modificare nu este interzisă de către politică.

Dacă o setare de aplicație de pe un computer client poate fi editată sau nu, acest lucru este determinat după prezența stării de „blocare” a setării în interiorul politicii:

- Dacă o setare este blocată () , nu poți edita local valoarea acestei setări. Valoarea setării specificată de către politică este folosită pentru toate computerele client din grupul de administrare.
- Atunci când o setare este deblocată () , poți edita local setarea. O setare configurată local este aplicată tuturor computerelor client din grupul de administrare. Setarea configurată de politică nu se aplică.

După aplicarea pentru prima dată a politicii, setările locale ale aplicației se modifică în conformitate cu setările de politică.

Drepturile de accesare a setărilor politicii (citire, scriere, executare) sunt specificate pentru fiecare utilizator care are acces la serverul de administrare Kaspersky Security Center și separat pentru fiecare domeniu operațional al Kaspersky Endpoint Security. Pentru a configura drepturile de acces la setările politicii, accesează secțiunea **Securitate** din fereastra de proprietăți a serverului de administrare Kaspersky Security Center.

Următoarele domenii operaționale ale Kaspersky Endpoint Security sunt evidențiate:

- Protecție antivirus. Domeniul operațional include Antivirus pentru fișiere, Antivirus pentru e-mail, Antivirus pentru Web, Antivirus MI, Scanare de vulnerabilități și activități de scanare.
- Componenta Control pornire aplicații. Domeniul operațional include componenta Application Startup Control.
- Componenta Control dispozitive. Domeniul operațional include componenta Control dispozitive.
- Criptare. Domeniul operațional include unitatea de hard disk, componente de criptare pentru fișiere și directoare.
- Zona de încredere. Domeniul operațional include Zona de încredere.
- Control Web. Domeniul operațional include componenta Control Web.
- Prevenire intruziuni. Acest domeniu operațional include Monitorizare activitate aplicație, Monitor de vulnerabilități, Firewall, Blocare atacuri de rețea și Control drepturi aplicații.
- Funcționalitate de bază. Acest domeniu operațional include setări generale ale aplicației care nu sunt specificate pentru alte domenii funcționale, inclusiv: licențiere, setări KSN, activități de inventar, activități de actualizare pentru baza de date și pentru modulele aplicației, Autoprotecție, setări avansate ale aplicației, rapoarte și zone de stocare, setări pentru protecția prin parolă și setări pentru interfața aplicației.

Poți efectua următoarele operațiuni cu o politică:

- Crearea unei politici.
- Editarea setărilor de politică.

Dacă contul de utilizator sub care ai accesat serverul de administrare nu are drepturi pentru editarea setărilor pentru anumite domenii funcționale, setările acestora nu sunt disponibile pentru editare.

- Ștergerea unei politici.

- Modificarea stării unei politici.

Pentru informații despre utilizarea politicilor care nu sunt legate de interacțiunea cu Kaspersky Endpoint Security, consultă *Ghidul administratorului Kaspersky Security Center*.

## Crearea unei politici

*Pentru a crea o politică:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. Efectuează una dintre următoarele acțiuni:
  - Selectează directorul **Dispozitive administrate** al arborelui consolei de administrare dacă dorești să creezi o politică pentru toate computerele gestionate de Kaspersky Security Center.
  - În directorul **Dispozitive administrate** al arborelui consolei de administrare, selectează directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Politici**.
4. Efectuează una dintre următoarele acțiuni:
  - Fă clic pe butonul **Creează o politică**.
  - Fă clic dreapta pentru a deschide meniul contextual și selectează **Creare Politică**.

Expertul de politică pornește.

5. Urmează instrucțiunile din Expertul de politică.

## Editarea setărilor de politică

*Pentru a edita setările politicii:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive administrate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare relevant pentru care dorești să editezi setările politicii.
3. În spațiul de lucru, selectează fila **Politici**.
4. Selectează politica necesară.
5. Deschide fereastra **Proprietăți: <Nume politică>** utilizând una dintre următoarele metode:



- În meniul contextual al politicii, selectează **Proprietăți**.
- Fă clic pe linkul **Configurare politică** în dreapta spațiului de lucru al Consolei de administrare.

Setările de politică pentru Kaspersky Endpoint Security 10 for Windows includ setările componentelor și [setările aplicației](#). Secțiunile **Protecție antivirus** și **Control endpoint** din fereastra **Proprietăți: <Nume politică>** afișează setările pentru componentele de protecție și control, secțiunea **Criptare date** afișează setările de criptare pentru fișiere și directoare, iar secțiunea **Setări avansate** afișează setările aplicației.

Pentru a activa afișarea setărilor de criptare a datelor și setările componentelor de control în setările de politică, trebuie să bifezi casetele de selectare corespunzătoare în fereastra **Setări interfață** a Kaspersky Security Center.

6. Editează setările politicii.

7. Pentru a salva modificările, în fereastra **Proprietăți: <Nume politică>**, fă clic pe **OK**.

## Selectarea setărilor care vor fi afișate în politica aplicației Kaspersky Security Center

*Pentru a selecta setările care vor fi afișate în politica aplicației Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.
2. În meniul contextual al nodului **Server de administrare – <Nume computer>** din arborele Consolei de administrare, selectează Vizualizare → **Setări interfață**.  
Se deschide fereastra **Setări interfață**.
3. În fereastra **Setări interfață**, bifează casetele de selectare de lângă setările care trebuie să fie afișate în setările de creare a politicii aplicației Kaspersky Security Center și în proprietățile politicii:
  - Bifează caseta de selectare **Afișare componente Control endpoint** pentru a activa afișarea setărilor pentru componentele de control în fereastra Expertului de politică nouă al Kaspersky Security Center și în proprietățile politicii.
  - Bifează caseta de selectare **Afișare criptare și protecție date** pentru a activa afișarea setărilor de criptare a datelor în Expertul de politică nouă al Kaspersky Security Center și în proprietățile politicii.
4. Fă clic pe **OK**.

# Trimiterea de mesaje ale utilizatorului către serverul Kaspersky Security Center

Un utilizator poate trimite un mesaj administratorului rețelei locale în următoarele cazuri:

- Componenta Control dispozitive a blocat accesul la dispozitiv.  
Șablonul de mesaj pentru solicitarea accesului la un dispozitiv blocat este disponibil în interfața Kaspersky Endpoint Security, în secțiunea [Control dispozitive](#).
- Componenta Control pornire aplicații a blocat pornirea unei aplicații.  
Șablonul de mesaj pentru a solicita permiterea pornirii unei aplicații blocate este disponibil în interfața Kaspersky Endpoint Security, în secțiunea [Control pornire aplicații](#).
- Componenta Control Web a blocat accesul la o resursă Web.  
Șablonul de mesaj pentru a solicita accesul la o resursă Web blocată este disponibil în interfața Kaspersky Endpoint Security, în secțiunea [Control Web](#).

Metoda folosită pentru trimiterea mesajelor și șablonul utilizat depinde de existența sau nu a unei politici active Kaspersky Security Center pe computerul pe care este instalată aplicația Kaspersky Endpoint Security și de existența sau nu a unei conexiuni cu serverul de administrare Kaspersky Security Center. Sunt posibile următoarele scenarii:

- Nu se execută o politică a aplicației Kaspersky Security Center pe computerul pe care este instalat Kaspersky Security Center: se trimite prin e-mail un mesaj al utilizatorului către administratorul rețelei locale.  
Câmpurile mesajului sunt populate din șablonul definit în interfața locală a Kaspersky Endpoint Security.
- Se execută o politică a aplicației Kaspersky Security Center pe computerul pe care este instalat Kaspersky Security Center: se trimite mesajul standard către serverul de administrare Kaspersky Security Center.  
În acest caz, mesajele utilizatorului sunt disponibile spre vizualizare în [spațiul de stocare pentru evenimente Kaspersky Security Center](#). Câmpurile mesajului sunt populate cu valori din câmpurile șablonului definit în politica aplicației Kaspersky Security Center.
- Dacă pe computerul pe care este instalată aplicația Kaspersky Endpoint Security este folosită o politică „absent de la birou” a Kaspersky Security Center, metoda folosită pentru trimiterea mesajelor depinde de existența sau nu a unei conexiuni la Kaspersky Security Center.
  - Dacă a fost stabilită o conexiune cu aplicația Kaspersky Security Center, Kaspersky Endpoint Security trimite mesajul standard către serverul de administrare Kaspersky Security Center.

- Dacă lipsește o conexiune cu Kaspersky Security Center, se trimite un mesaj al utilizatorului către administratorul rețelei locale, prin e-mail.

În ambele cazuri, câmpurile mesajului sunt populate cu valori din câmpurile șablonului definit în politica aplicației Kaspersky Security Center.

## Vizualizarea mesajelor utilizatorului în spațiul de stocare a evenimentelor din Kaspersky Security Center

Componentele [Control pornire aplicații](#), [Control dispozitive](#) și [Control Web](#) permit utilizatorilor computerelor din rețeaua LAN pe care este instalat Kaspersky Endpoint Security să trimită mesaje către administrator.

Un utilizator poate trimite mesaje către administrator folosind două metode:

- Ca eveniment în spațiul de stocare a evenimentelor din Kaspersky Security Center.

Un eveniment de utilizator este trimis către zona de stocare a evenimentelor din Kaspersky Security Center atunci când aplicația Kaspersky Endpoint Security instalată pe computerul utilizatorului funcționează în baza unei politici active.

- Ca mesaj de e-mail.

Informațiile de utilizator sunt trimise prin e-mail dacă aplicația Kaspersky Endpoint Security instalată pe computerul utilizatorului nu execută o politică sau execută o politică „absent de la birou”.

*Pentru a vizualiza un mesaj de la un utilizator în spațiul de stocare a evenimentelor din Kaspersky Security Center:*

1. Deschide consola de administrare a Kaspersky Security Center.

2. În nodul **Server de administrare** din arborele consolei de administrare, selectează fila **Evenimente**.

Spațiul de lucru Kaspersky Security Center afișează toate evenimentele apărute în cursul funcționării Kaspersky Endpoint Security, inclusiv mesaje primite de administrator de la utilizatorii rețelei LAN.

3. Pentru a configura filtrul de evenimente, în lista verticală **Selectare evenimente**, selectează **Solicitare utilizator**.

4. Selectează mesajul de trimis către administrator.

5. Deschide fereastra **Setări eveniment** într-unul din următoarele două moduri:

- Fă clic dreapta pe eveniment. În meniul contextual care se deschide, selectează **Proprietăți**.

- Fă clic butonul **Deschide fereastra de proprietăți a evenimentului** în partea dreaptă a spațiului de lucru Consolă de administrare.

## Participarea la Kaspersky Security Network

Această secțiune conține informații despre participarea la Kaspersky Security Network și instrucțiuni pentru modul de activare sau dezactivare a serviciului Kaspersky Security Network.

## Despre participarea la Kaspersky Security Network

Pentru a-ți proteja mai eficient computerul, Kaspersky Endpoint Security folosește informații adunate de la utilizatori de pe întregul glob. *Kaspersky Security Network* este conceput pentru a colecta aceste date.


Kaspersky Security Network (KSN) este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false.

În funcție de locația infrastructurii, există un serviciu KSN global (infrastructura este găzduită de serverele Kaspersky) și un serviciu KSN privat (infrastructura este găzduită de servere de la terți, de exemplu în rețeaua furnizorului de servicii Internet).

După schimbarea licenței, trimite detaliile noii chei către furnizorul de servicii pentru a putea folosi serviciul KSN privat. În caz contrar, schimbul de date cu KSN nu va fi posibil.

Grație utilizatorilor care participă la KSN, Kaspersky poate primi cu promptitudine informații despre tipuri și surse ale noilor amenințări, poate dezvolta soluții pentru neutralizarea acestora și poate minimiza numărul de alarme false afișate de componentele aplicației.

În cursul participării la KSN, aplicația trimite în mod automat statistici generate în cursul funcționării aplicației către KSN. Aplicația poate de asemenea să trimită anumite fișiere (sau părți de fișiere) pe care hackerii le pot folosi pentru a dăuna computerului sau datele către Kaspersky, pentru scanare suplimentară.

Nu sunt colectate, procesate sau stocate date personale. Pentru informații mai detaliate despre trimiterea informațiilor statistice Kaspersky generate în cursul participării la KSN și despre stocarea și distrugerea acestor informații, consultă Declarația Kaspersky Security Network și [site-ul Web Kaspersky](#) . Fișierul ksn\_<language ID>.txt care conține textul Declarației Kaspersky Security Network este inclus în kitul de distribuție a aplicației.

Pentru a reduce încărcarea serverelor KSN, Kaspersky este posibil să lanseze baze de date antivirus care dezactivează temporar sau care restricționează parțial accesul la Kaspersky Security Network. În acest caz, [starea conexiunii la KSN](#) va apărea ca [Activată cu restricții](#).

Computerele utilizatorilor administrate de Serverul de administrare Kaspersky Security Center pot interacționa cu KSN prin serviciul Proxy KSN.

Serviciul Proxy KSN oferă următoarele funcționalități:

- Computerul utilizatorului poate interoga KSN și poate trimite informații către KSN, chiar și fără acces direct la Internet.
- KSN Proxy stochează în memoria cache datele procesate, reducând astfel încărcarea conexiunii de rețea externe și accelerând recepția informațiilor solicitate de către computerul utilizatorului.

Mai multe detalii despre serviciul Proxy KSN pot fi găsite în *Ghidul administratorului Kaspersky Security Center*.

Setările serviciului Proxy KSN pot fi configurate în proprietățile politicii [Kaspersky Security Center](#).

Participarea la Kaspersky Security Network este voluntară. Aplicația îl invită pe utilizator să participe la KSN în cursul configurării inițiale a aplicației. Utilizatorii pot începe sau pot întrerupe participarea la KSN în orice moment.

## Activarea și dezactivarea utilizării serviciului Kaspersky Security Network

*Pentru a activa sau a dezactiva utilizarea serviciului Kaspersky Security Network:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, în secțiunea **Setări avansate**, selectează subsecțiunea **Setări KSN**.  
Setările serviciului Kaspersky Security Network se afișează în partea dreaptă a ferestrei.
3. Efectuează una dintre următoarele acțiuni:
  - Dacă dorești să activezi utilizarea Kaspersky Security Network, bifează caseta de selectare **Accept Declarația KSN și termenii de participare**.
  - Dacă dorești să dezactivezi utilizarea Kaspersky Security Network, debifează caseta de selectare **Accept Declarația KSN și termenii de participare**.

4. Pentru a salva modificările, fă clic pe butonul **Salvare**.

## Verificarea conexiunii la serviciul Kaspersky Security Network

*Pentru a verifica o conexiune la serviciul Kaspersky Security Network:*

1. Deschide [fereastra principală a aplicației](#).

2. În partea sus a ferestrei, fă clic pe butonul **Kaspersky Security Network**.

Se deschide fereastra **Kaspersky Security Network**.

În stânga ferestrei **Kaspersky Security Network** este afișat modul de conectare la Kaspersky Security Network, sub forma unui buton rotund **KSN**:

- Dacă aplicația Kaspersky Endpoint Security nu este conectată la Kaspersky Security Network, butonul **KSN** are culoarea gri. Starea prezentată sub butonul **KSN** este *Dezactivat*.
- Dacă aplicația Kaspersky Endpoint Security este conectată la Kaspersky Security Network și serverele KSN sunt disponibile, butonul **KSN** are culoarea verde. Următoarele informații apar sub butonul **KSN**: starea *Activat*, tipul de KSN în uz – **KSN privat** sau **KSN global** și data și ora ultimei sincronizări cu serverele KSN. Partea dreaptă a ferestrei afișează statistici despre reputația fișierelor, resurselor Web și programelor software.

Kaspersky Endpoint Security adună date statistice despre utilizarea KSN atunci când deschizi fereastra **Kaspersky Security Network**. Statisticile nu sunt actualizate în timp real.

- Dacă aplicația Kaspersky Endpoint Security este conectată la Kaspersky Security Network, dar serverele KSN nu sunt disponibile, butonul **KSN** are culoarea roșie. Starea prezentată sub butonul **KSN** este *Activat*.

Dacă ora ultimei sincronizări cu serverele KSN este cu mai mult de 15 minute în urmă sau are starea *Necunoscut*, aceasta înseamnă că serverele KSN nu sunt disponibile. În acest caz, ți se recomandă să contactezi asistența tehnică sau furnizorul de servicii.

O conexiunea la serverele Kaspersky Security Network poate lipsi din următoarele motive:

- Computerul nu este conectat la Internet.
- Aplicația nu a fost activată sau licența a expirat.
- Au fost detectate probleme legate de cheie (de exemplu, cheia a fost introdusă în lista neagră).

## Verificarea reputației unui fișier în Kaspersky Security Network

Serviciul KSN îți permite să recuperezi informații despre aplicațiile care sunt incluse în bazele de date de reputație Kaspersky. Aceasta permite o gestionare flexibilă a politicilor de pornire a aplicațiilor la nivelul companiei, împiedicând astfel pornirea unor adware și alte programe care pot fi folosite de către infractori pentru a aduce daune computerului sau datelor personale.

*Pentru a verifica reputația unui fișier în Kaspersky Security Network:*

1. Fă clic dreapta pentru a afișa meniul contextual al fișierului a cărui reputație dorești s-o verifici.
2. Selectează opțiunea **Verifică reputația în KSN**.

Această opțiune este disponibilă dacă ai acceptat termenii din [Declarația Kaspersky Security Network](#).

Această acțiune deschide fereastra **<Nume fișier> - Reputație în KSN**. Fereastra **<Nume fișier> - Reputație în KSN** afișează următoarele informații despre fișierul verificat:

- **Cale**. Calea în care fișierul este salvat pe disc.
- **Versiune**. Versiunea aplicației (informația aceasta este afișată numai pentru fișiere executabile).
- **Semnătură digitală**. Prezența unei semnături digitale pentru fișier.
- **Semnat**. Data la care a fost semnat certificatul cu o semnătură digitală.
- **Creat**. Data creării fișierului.
- **Modificat**. Data ultimei modificări a fișierului.
- **Dimensiune**. Spațiul-disc ocupat de fișier.
- Informații despre câți utilizatori au încredere în fișier sau îl blochează.

## Protecție îmbunătățită cu Kaspersky Security Network

Kaspersky oferă un nivel suplimentar de protecție pentru utilizatori prin intermediul Kaspersky Security Network. Această metodă de protecție este adresată combaterii amenințărilor complexe și atacurilor de tip Ziua 0. Tehnologiile cloud integrate și experiența analiștilor de viruși de la Kaspersky fac din aplicația Kaspersky Endpoint Security o opțiune inegalabilă pentru protecția împotriva celor mai sofisticate amenințări de rețea.

Detalii despre protecția îmbunătățită din Kaspersky Endpoint Security sunt disponibile pe site-ul Web Kaspersky.

## Surse de informații despre aplicație

### Pagina Kaspersky Endpoint Security pe site-ul Web Kaspersky

În [pagina Kaspersky Endpoint Security](#), poți vedea informații generale despre aplicație și despre funcțiile și caracteristicile ei.

Pagina Kaspersky Endpoint Security conține un link către magazinul online. Aici poți să achiziționezi sau să îți reînnoiești licența pentru aplicație.

### Pagina Kaspersky Endpoint Security din Baza de cunoștințe

*Baza de cunoștințe* este o secțiune de pe site-ul Web de Asistență tehnică.

În [pagina Kaspersky Endpoint Security din Baza de cunoștințe](#), poți citi articole care oferă informații folositoare, recomandări și răspunsuri la întrebări frecvente despre cum să achiziționezi, să instalezi și să utilizezi aplicația.

Articolele din Baza de cunoștințe pot răspunde la întrebări care nu sunt legate doar de Kaspersky Endpoint Security, ci și de alte aplicații Kaspersky. Articolele din Baza de cunoștințe pot conține, de asemenea, noutăți de la serviciul de Asistență tehnică.

### Discutarea aplicațiilor Kaspersky pe Forumul utilizatorilor

Dacă întrebarea ta nu necesită un răspuns urgent, o poți discuta cu experții Kaspersky și cu alți utilizatori pe [forumul](#) nostru.

Pe acest forum poți vizualiza subiecte existente, poți trimite comentarii și poți crea subiecte de discuții noi.

## Contactarea Serviciului de asistență tehnică

Această secțiune descrie modurile în care poți primi asistență tehnică și condiții în baza cărora aceasta este disponibilă.

## Cum se obține asistență tehnică



Dacă nu găsești o soluție pentru problema ta în documentația aplicației sau într-una dintre [sursele de informații despre aplicație](#), îți recomandăm să contactezi Serviciul de asistență tehnică. Specialiștii de la Serviciul de asistență tehnică vor răspunde la întrebările tale despre instalarea și utilizarea aplicației.

Asistența tehnică este disponibilă numai pentru utilizatorii care au achiziționat o licență comercială. Utilizatorii care au primit o licență trial nu au dreptul la asistență tehnică.

Înainte de a contacta Asistența tehnică, vă rugăm să citiți [regulile pentru asistență](#).

Poți contacta Serviciul de asistență tehnică în următoarele două moduri:

- [Apelând Asistența tehnică prin telefon](#)
- Trimițând o solicitare către Asistență tehnică Kaspersky prin [portalul Kaspersky CompanyAccount](#)

## Asistența tehnică prin telefon

Poți apela reprezentanți ai serviciului de Asistență tehnică din majoritatea regiunilor din lume. Află informații despre cum să primești asistență tehnică și regiunea ta și date de contact pentru serviciul de Asistență tehnică pe [site-ul Web al serviciului de Asistență tehnică Kaspersky](#).

Înainte de a contacta Asistența tehnică, vă rugăm să citiți [regulile pentru asistență](#).

## Asistența tehnică prin Kaspersky CompanyAccount


[Kaspersky CompanyAccount](#) este un portal pentru companiile care folosesc aplicații Kaspersky. Portalul Kaspersky CompanyAccount este conceput să faciliteze interacțiunea dintre utilizatori și experți Kaspersky prin intermediul solicitărilor electronice. Poți folosi portalul Kaspersky CompanyAccount pentru a urmări starea solicitărilor tale electronice și a stoca un istoric al acestor solicitări.

Îți poți înregistra pe toți angajații organizației tale într-un singur cont Kaspersky CompanyAccount. Dacă ai un singur cont, poți să gestionezi centralizat solicitările electronice de la angajații înregistrați pe Kaspersky și poți să administrezi drepturile acestor angajați prin Kaspersky CompanyAccount.

Portalul Kaspersky CompanyAccount este disponibil în următoarele limbi:

- Engleză
- Spaniolă

- Italiană
- Germană
- Poloneză
- Portugheză
- Rusă
- Franceză
- Japoneză

Pentru a afla mai multe despre Kaspersky CompanyAccount, vizitează [site-ul Web de Asistență tehnică](#) .

## Colectarea de informații pentru serviciul de asistență tehnică

După ce îi informezi pe specialiștii Serviciului de asistență tehnică Kaspersky despre problema ta, este posibil să îți ceară să creezi un *fișier de urmărire*. Fișierul de urmărire permite urmărirea procesului prin care se execută comenzile aplicației pas cu pas și se stabilește etapa din funcționarea aplicației în care apare eroarea.

Specialiștii Serviciului de asistență tehnică pot solicita, de asemenea, informații suplimentare despre sistemul de operare, procesele care se execută pe computer, rapoarte detaliate despre funcționarea componentelor aplicației și imagini ale blocajelor aplicațiilor.

Poți colecta informațiile necesare cu ajutorul aplicației Kaspersky Endpoint Security. Informațiile colectate pot fi salvate pe unitatea de hard disk și încărcate ulterior, la un moment convenabil.

Atunci când execuți diagnosticarea, experții serviciului de Asistență tehnică este posibil să-ți solicite să modifice setările aplicației astfel:

- Activarea funcționalității care colectează informațiile de diagnosticare.
- Ajustarea unor setări ale componentelor individuale ale aplicației care nu sunt disponibile în interfața de utilizator standard.
- Modificarea setărilor pentru depozitarea și transmisia informațiilor de diagnosticare colectate.
- Configurarea interceptării și înregistrării în jurnal a traficului de rețea.

Experții serviciului de Asistență tehnică îți vor furniza toate informațiile necesare pentru a efectua aceste operațiuni (descrierea secvenței de pași, setările de modificat, fișiere de configurare, scripturi, funcționalitate suplimentară în linia de comandă, module de depanare, utilitare speciale etc.) și te vor informa ce date sunt colectate în scopul depanării. Informațiile detaliate colectate pentru diagnosticare sunt salvate pe computerul utilizatorului. Datele colectate nu sunt trimise automat către Kaspersky.

Setările folosite pentru a determina adresa serverului pentru trimiterea fișierelor imagine către Kaspersky sunt stocate pe computerul utilizatorului. Dacă este necesar, valorile pentru aceste setări pot fi editate în cheia de registru pentru sistemul de operare  
`"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

Operațiunile prezentate mai sus trebuie efectuate numai sub supravegherea specialiștilor din departamentul de Asistență tehnică, în conformitate cu instrucțiunile acestora. Modificările nesupravegheate în setările aplicației efectuate altminteri decât este descris în Ghidul administratorului sau în instrucțiunile specialiștilor departamentului de Asistență tehnică pot duce la încetinirea sau blocarea sistemului de operare, pot afecta securitatea computerului sau pot compromite disponibilitatea și integritatea datelor procesate.

## Crearea unui fișier de urmărire

*Pentru a crea un fișier de urmărire:*

1. Deschide [fereastra principală a aplicației](#).

2. În fereastra principală a aplicației, fă clic pe butonul .

Se deschide fereastra **Asistență**.

3. În fereastra **Asistență**, fă clic pe butonul **Urmărire sistem**.

Se deschide fereastra **Informații pentru Serviciul de asistență tehnică**.

4. Pentru a începe procesul de urmărire, bifează caseta de selectare **Activare urmărire**.

5. În lista verticală **Nivel**, selectează nivelul de urmărire.

Se recomandă clarificarea nivelului de urmărire necesar cu un special al Serviciului de asistență tehnică. În lipsa asistenței din partea Serviciului de asistență tehnică, setează nivelul de urmărire la **Normal (500)**.

6. Reprodu situația în care a apărut problema.

7. Pentru a opri procesul de urmărire, revino la fereastra **Informații pentru Serviciul de asistență tehnică** și debifează caseta de selectare **Activare urmărire**.

După crearea fișierului de urmărire, poți continua cu [încărcarea rezultatelor urmăririi pe serverul Serviciului de asistență tehnică](#).

## Conținutul și zona de stocare pentru fișierele de urmărire

Utilizatorul este direct răspunzător pentru asigurarea siguranței datelor colectate, în special pentru monitorizarea și restricționarea accesului la datele colectate stocate pe computer până când acestea sunt trimise către Kaspersky.

Fișierele de urmărire sunt stocate pe computerul tău într-o formă modificată, care nu poate fi citită cât timp aplicația este în uz, și sunt permanent șterse atunci când aplicația este eliminată.

Fișierele de urmărire sunt stocate în directorul ProgramData\Kaspersky Lab.

Fișierul de urmărire are următorul format de nume: KES<număr versiune\_datăXX.XX\_orăXX.XX\_idprocesXXX.><tip fișier urmărire>.log.enc1.

Fișierul de urmărire pentru Agentul de Autentificare este stocat în directorul Informații volum sistem și are următorul nume: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.

Poți vizualiza datele salvate în fișierele de urmărire. Contactează serviciul de asistență tehnică al Kaspersky pentru sfaturi privind vizualizarea datelor.

Toate fișierele de urmărire conține următoarele date comune:

- Oră eveniment.
- Numele firului de execuție.

Fișierul de urmărire pentru Agentul de Autentificare nu conține aceste informații.

- Componenta aplicației care a determinat evenimentul.
- Gradul de gravitate a evenimentului (eveniment informațional, avertizare, eveniment critic, eroare).
- O descriere a evenimentului implicând executarea comenzii de către o componentă a aplicației și rezultatul executării acestei comenzi.

## Conținutul fișierelor de urmărire SRV.log, GUI.log și ALL.log

Fișierele de urmărire SRV.log, GUI.log și ALL.log pot stoca următoarele informații, pe lângă datele generale:

- Date personale, inclusiv nume de familie, prenume și al doilea prenume, dacă aceste date sunt incluse în calea către fișiere de pe computerul local.
- Numele de utilizator și parola, dacă au fost transmise necodate. Aceste date pot fi înregistrate în fișierele de urmărire în cursul scanării traficului Internet. Traficul este înregistrat în fișierele de urmărire numai de la trafmon2.ppl.
- Numele de utilizator și parola, dacă sunt incluse în anteturile HTTP.
- Numele contului Microsoft Windows, dacă acesta este inclus într-un nume de fișier.
- Adresa ta de e-mail sau o adresă Web care conține numele contului tău și parola, dacă acestea sunt incluse în numele obiectului detectat.
- Site-uri Web pe care le vizitezi și redirectionări de la aceste site-uri Web. Aceste date sunt scrise în fișiere de urmărire atunci când aplicația scanează site-uri Web.
- Adresa serverului proxy, numele computerului, adresa IP și numele de utilizator folosit pentru conectare la serverul proxy. Aceste date sunt scrise în fișiere de urmărire dacă aplicația folosește un server proxy.
- Adrese IP la distanță la care a stabilit conexiuni computerul tău.
- Subiectul mesajului, ID-ul, numele expeditorului și adresa paginii Web a expeditorului mesajului de pe o rețea socială. Aceste date sunt scrise în fișiere de urmărire dacă este activată componenta Control Web.

## Conținutul fișierelor de urmărire HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Pe lângă datele generale, fișierul de urmărire HST.log conține informații despre executarea unei activități de actualizare a bazei de date și a modulelor aplicației.

Pe lângă datele generale, fișierul de urmărire BL.log conține informații despre evenimente apărute în cursul funcționării aplicației, precum și date necesare pentru depanarea erorilor aplicației. Acest fișier este creat dacă aplicația este lansată cu parametrul avp.exe -bl.

Pe lângă datele generale, fișierul de urmărire Dumpwriter.log conține informații despre serviciu necesare pentru depanarea erorilor apărute atunci când este scris fișierul de imagine al aplicației.

Pe lângă datele generale, fișierul de urmărire WD.log conține informații despre evenimente apărute în cursul funcționării serviciului avpsus, inclusiv eveniment legate de actualizarea modulelor aplicației.

Pe lângă datele generale, fișierul de urmărire AVPCon.dll.log conține informații despre evenimente apărute în cursul funcționării modulului de conectivitate al Kaspersky Security Center.

## Conținutul fișierelor de urmărire pentru plug-inurile aplicației

Fișierele de urmărire pentru plug-inurile aplicației conțin, pe lângă datele generale, următoarele informații:

- Fișierul de urmărire shellex.dll.log al plug-inului care pornește activitatea de scanare din meniul contextual conține informații despre executarea activității de scanare și date necesare pentru depanarea plug-inului.
- Fișierul de urmărire mcou.OUTLOOK.EXE al plug-inului Antivirus pentru e-mail poate conține părți din mesaje de e-mail, inclusiv adrese de e-mail.

## Conținutul fișierului de urmărire pentru Agentul de Autentificare

Pe lângă datele generale, fișierul de urmărire pentru Agentul de Autentificare conține informații despre funcționarea Agentului de Autentificare și despre acțiunile efectuate de către utilizator cu Agentul de Autentificare.

## Activarea sau dezactivarea transmiterii către Kaspersky a fișierelor imagine memorie și a fișierelor de urmărire

*Pentru a sau a dezactiva transmiterea către Kaspersky a fișierelor imagine memorie și a fișierelor de urmărire:*

1. Deschide [fereastra cu setările aplicației](#).
2. În partea stângă a ferestrei, selectează secțiunea **Setări avansate**.  
Setările avansate ale aplicației se afișează în partea dreaptă a ferestrei.
3. În secțiunea **Mod de funcționare**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Mod de funcționare**.
4. În fereastra **Mod de funcționare**, bifează caseta de selectare **Activare scriere imagine** pentru a permite aplicației să scrie fișiere imagine ale aplicațiilor.
5. Efectuează una dintre următoarele acțiuni:
  - Bifează caseta de selectare **Trimite fișiere imagine și de urmărire la Kaspersky** dacă dorești ca aplicația să afișeze o solicitare în fereastra **Încărcare informații pe server**

**pentru Serviciul de asistență tehnică** pentru a trimite către Kaspersky fișiere imagine și fișiere de urmărire pentru a analiza cauzele erorilor la următoarea pornire a aplicației.

- În caz contrar, debifează caseta de selectare **Trimite fișiere imagine și de urmărire la Kaspersky**.

6. Fă clic pe **OK** în fereastra **Mod de funcționare**.

7. Pentru a salva modificările, fă clic pe butonul **Salvare** în fereastra principală a aplicației.

## Trimiterea de fișiere către serverul serviciului de Asistență tehnică

Fișierele care conțin informații despre sistemul de operare, fișierele de urmărire și fișierele imagine memorie trebuie trimise către experții serviciului de Asistență tehnică al Kaspersky.

*Pentru a trimite fișiere către serverul serviciului de Asistență tehnică:*

1. Repornește Kaspersky Endpoint Security după orice disfuncționalitate în operarea sa.

Această acțiune deschide fereastra **Precedenta lansare a aplicației nu a reușit**.

Fereastra **Precedenta lansare a aplicației nu a reușit** se va deschide de fiecare dată când Kaspersky Endpoint Security este pornit (inclusiv după repornirea computerului), până când trimiți fișierele imagine memorie sau fișierele de urmărire către serviciul Asistență tehnică sau faci clic pe butonul **Nu trimite**.

2. În fereastra **Precedenta lansare a aplicației nu a reușit**, deschide lista de fișiere generate făcând clic pe **aici**.

3. Bifează casetele din dreptul fișierelor pe care dorești să le trimiți către serviciul de Asistență tehnică.

4. Fă clic pe butonul **Afișare text Declarație**.

Se deschide fereastra **Declarație privind furnizarea datelor**.

5. Citește textul Declarației privind furnizarea datelor și fă clic pe butonul **Închidere**.

6. În fereastra **Precedenta lansare a aplicației nu a reușit**, bifează caseta de selectare **Sunt de acord cu Declarația referitoare la furnizarea datelor**.

7. Fă clic pe butonul **Trimitere**.

Această acțiune deschide fereastra **Număr solicitare**.

8. În fereastra **Număr solicitare**, specifică numărul atribuit solicitării tale atunci când ai contactat serviciul de Asistență tehnică prin Kaspersky CompanyAccount.

9. Fă clic pe **OK**.

Fișierele de date selectate sunt arhivate și trimise către servul Serviciului de asistență tehnică.

## Activarea și dezactivarea protecției pentru fișierele imagine și de urmărire

Fișierele imagine și de urmărire conțin informații despre sistemul de operare, precum și [date confidentiale ale utilizatorului](#). Pentru a împiedica accesul neautorizat la aceste date, poți activa protecția fișierelor imagine și de urmărire.

Dacă este activată protecția fișierelor imagine și de urmărire, fișierele pot fi accesate de către următorii utilizatori:

- Fișierele imagine pot fi accesate de către administratorul de sistem și administratorul local, precum și de către utilizatorul care a activat scrierea fișierelor imagine și de urmărire.
- Fișierele de urmărire pot fi accesate numai de către administratorul de sistem și administratorul local.

*Pentru a activa și a dezactiva protecția pentru fișierele imagine și de urmărire:*

1. Deschide [fereastra cu setările aplicației](#).
2. Selectează secțiunea **Setări avansate** în stânga.  
Setările aplicației sunt afișate în dreapta ferestrei.
3. În secțiunea **Mod de funcționare**, fă clic pe butonul **Setări**.  
Se deschide fereastra **Mod de funcționare**.
4. Efectuează una dintre următoarele acțiuni:
  - Bifează caseta de selectare **Activare protecție fișiere imagine memorie și de urmărire**, dacă dorești să activezi protecția.
  - Debifează caseta de selectare **Activare protecție fișiere imagine memorie și de urmărire**, dacă dorești să dezactivezi protecția.
5. Fă clic pe **OK** în fereastra **Mod de funcționare**.
6. Pentru a salva modificările, fă clic pe butonul **Salvare** în fereastra principală a aplicației.



Fișierele de imagine și cele de urmărire care au fost scrise cât timp protecția este activă vor rămâne protejate și după dezactivarea acestei funcții.

## Glosar

### Activitate

Funcții efectuate de aplicația Kaspersky ca activități, de exemplu: Protecție în timp real pentru fișiere, Scanare completă dispozitive, Actualizare bază de date.

### Actualizare

Procedură de înlocuire sau adăugare de fișiere noi (baze de date sau module ale aplicației) primite de la serverele Kaspersky.

### Adresă normalizată pentru o resursă Web

Forma normalizată a adresei unei resurse Web este o reprezentare textuală, obținută prin normalizare, a adresei resursei Web. Normalizarea este un proces prin care reprezentarea textuală a adresei resursei Web este modificată în conformitate cu anumite reguli (de exemplu, excluderea numelui de conectare HTTP, a parolei și a portului de conectare din reprezentarea textuală a adresei resursei Web; de asemenea, adresa resursei Web este modificată din caractere majuscule în caractere minuscule).

În contextul protecției antivirus, scopul normalizării adresei unei resurse Web este evitarea scanării adreselor de site-uri Web care pot diferi ca sintaxă deși sunt echivalente fizic.

Exemplu:

Formă nenormalizată a unei adrese: `www.Exemplu.com\.`

Formă normalizată a unei adrese: `www.exemplu.com\.`

### Agent de autentificare

O interfață pentru parcurgerea procesului de autentificare în vederea accesării unor unități hard disc criptate și încărcării sistemului de operare după criptarea unității hard disc pe care se află sistemul.

### Agent de rețea

O componentă Kaspersky Security Center care permite interacțiunea dintre serverul de administrare și aplicațiile Kaspersky care sunt instalate într-un nod de rețea specific (stație de lucru sau server). Această componentă este comună pentru toate aplicațiile Kaspersky care se execută în Windows. Versiunile dedicate de Agent de rețea sunt destinate aplicațiilor care se execută în alte sisteme de operare.

## Alarmă falsă

O alarmă falsă apare atunci când aplicația Kaspersky raportează un fișier neinfestat ca fiind infestat, deoarece semnătura fișierului este asemănătoare cu aceea a unui virus.

## Amprentă certificat

Informații folosite pentru a identifica o cheie de certificat. Se creează o amprentă aplicând o funcție hash criptografică valorii cheii.

## Analiză euristică

Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut.

## Analiză semnături

O tehnologie de detectare a amenințărilor care utilizează bazele de date Kaspersky Endpoint Security, ce conțin descrieri ale amenințărilor cunoscute și metode de eradicare a acestor amenințări. Protecția care utilizează analiza semnăturilor asigură un nivel de securitate minim acceptabil. În urma recomandărilor experților Kaspersky, această metodă este activată în permanență.

## Arhivă

Unul sau mai multe fișiere împachetate într-un singur fișier comprimat. Pentru împachetarea și despachetarea datelor este necesară o aplicație specializată denumită arhivator.

## Bază de date de adrese Web de phishing

O listă de adrese Web pe care specialiștii Kaspersky le-au stabilit ca fiind legate de activitatea de phishing. Baza de date este actualizată cu regularitate și face parte din kitul de distribuție a aplicației Kaspersky.

## Bază de date de adrese Web periculoase

O listă de adrese Web al căror conținut poate fi considerat periculos. Lista este creată de specialiștii Kaspersky. Ea este actualizată cu regularitate și este inclusă în kitul de distribuție a aplicației Kaspersky.

## Baze de date antivirus

Baze de date care conțin informații despre amenințările la adresa securității computerului cunoscute de Kaspersky la momentul lansării bazei de date antivirus. Semnăturile din baza de date antivirus ajută la detectarea codului rău intenționat din obiectele scanate. Bazele de date antivirus sunt create de specialiștii Kaspersky și sunt actualizate din oră în oră.

## Carantină

Kaspersky Endpoint Security plasează fișierele probabil infectate în acest director. Fișierele din Carantină sunt stocate în formă criptată.

## Certificat

Document electronic care conține cheia privată și informații despre proprietarul cheii și despre domeniul cheii și care confirmă faptul că această cheie publică aparține proprietarului. Certificatul trebuie să fie semnat de către centrul de certificare care l-a emis.

## Certificat licență

Un document pe care Kaspersky îl transferă utilizatorului odată cu fișierul cheie sau codul de activare. Conține informații despre licența acordată utilizatorului.

## Cheie activă

O cheie care este utilizată curent de aplicație.

## Cheie suplimentară

O cheie care certifică dreptul de utilizare a aplicației, însă care nu este utilizată în prezent.

## Conector agent de rețea

Funcționalitate a aplicației care conectează aplicația cu Agentul de rețea. Agentul de rețea permite administrarea la distanță a aplicației prin Kaspersky Security Center.

## Copie de rezervă

O zonă specială de stocare pentru copiile de rezervă ale fișierelor create înainte de încercarea dezinfectării sau a ștergerii.

## Corecție

O mică adăugire la aplicație care remediază erori descoperite în cursul funcționării aplicației sau care instalează actualizări.

## Dezinfectare

O metodă de procesare a obiectelor infectate, care conduce la recuperarea totală sau parțială a datelor. Nu toate obiectele infectate pot fi dezinfectate.

## Domeniu de protecție

Obiectele care sunt scanate constant de către protecția antivirus atunci când aceasta se execută. Proprietățile domeniilor de protecție diferă de la o componentă la alta.

## Domeniu de scanare

Obiectele pe care le scanează aplicația Kaspersky Endpoint Security atunci când efectuează o activitate de scanare.

## Emitent certificat

Centrul de certificare care a emis certificatul.

## Exploit

Programează cod care utilizează o vulnerabilitate în sistem sau software. Exploiturile sunt frecvent utilizate pentru a instala programe malware pe computer fără știința utilizatorului.

## Fișier infectabil

Un fișier care, din cauza structurii sau formatului său, poate fi utilizat de intruși ca „recipient” pentru stocarea și răspândirea de cod rău intenționat. De regulă, acesta este un fișier executabil, cu extensia .com, .exe sau .dll. Riscul de pătrundere a codului rău intenționat în astfel de fișiere este destul de ridicat.

## Fișier infectat

Un fișier care conține cod rău intenționat (cod al unui malware cunoscut detectat la scanarea fișierului). Kaspersky nu recomandă utilizarea unor astfel de fișiere, deoarece pot infecta computerul.

## Fișier probabil infectat

Un fișier care conține fie cod modificat al unui virus cunoscut, fie cod care seamănă cu cel al unui virus, însă nu este cunoscut încă de Kaspersky. Fișierele probabil infectate sunt detectate de Analizorul euristic.

## Grup de administrare

Un set de dispozitive care partajează funcții comune și un set de aplicații Kaspersky instalate pe ele. Dispozitivele sunt grupate astfel încât pot fi gestionate convenabile ca o singură unitate. Un grup poate include alte grupuri. Este posibilă crearea de politici de grup și activități de grup pentru fiecare aplicație instalată din grup.

## Listă neagră de adrese

O listă de adrese de e-mail de la care toate mesajele primite sunt blocate de către aplicația Kaspersky, indiferent de conținutul mesajului.

## Manager de fișiere portabil

Aceasta este o aplicație care furnizează o interfață pentru lucrul cu fișiere criptate de pe unități amovibile atunci când pe computer nu este disponibilă nicio funcționalitate de criptare.

## Mască de fișier

Reprezentarea numelui și a extensiei unui fișier utilizând metacaractere.

Măștile de fișier pot conține orice caractere permise în numele de fișiere, inclusiv metacaractere:

- \* – Înlocuiește orice zero sau mai multe caractere.
- ? – Înlocuiește orice caracter individual.

Reține că numele fișierului și extensia fișierului sunt separate întotdeauna prin punct.

## Modulele aplicației

Fișiere care sunt incluse în fișierul de instalare a aplicației, care implementează funcționalitatea de bază a aplicației. Un modul executabil separat corespunde fiecărui tip de activitate efectuată de aplicație (Protecție în timp real, Scanare la cerere și Actualizare). Atunci când se începe o scanare completă a computerului din fereastra principală a aplicației, inițializați modulul acestei activități.

## Mutarea fișierelor în Carantină

O metodă de gestionare a unui fișier probabil infectat prin care accesul la fișier este blocat și fișierul este mutat din locația sa originală în directorul Carantină, unde este păstrat în format criptat, pentru a elimina orice amenințare de infectare.

## Obiect OLE

Un fișier atașat sau un fișier încorporat într-un alt fișier. Aplicațiile Kaspersky permit scanarea obiectelor OLE pentru identificarea virușilor. De exemplu, dacă inserați un tabel Microsoft Office Excel într-un document Microsoft Office Word, tabelul este scanat ca obiect OLE.

## Phishing

Un tip de fraudă pe Internet în care sunt trimise mesaje e-mail cu scopul de a fura informații confidențiale, cel mai adesea date financiare.

## Server de administrare

O componentă a aplicației Kaspersky Security Center care stochează într-un punct central informațiile despre toate aplicațiile Kaspersky instalate în rețeaua companiei. Poate fi folosită și pentru gestionarea acestor aplicații.

## Serviciu de rețea

Set de parametri care definesc activitatea de rețea. Pentru această activitate de rețea poți crea o regulă de rețea care reglementează funcționarea componentei Firewall.

## Setări pentru activitate

Setări pentru aplicație, specifice pentru fiecare tip de activități.

## Setări pentru aplicație

Setările pentru aplicații sunt comune pentru toate tipurile de activități și guvernează funcționarea globală a aplicației, cum ar fi setările pentru performanța aplicației, setările pentru rapoarte și setările pentru copierea de rezervă.

## Subiect certificat

Deținătorul unei chei private legate de un certificat. Această persoană poate fi un utilizator, o aplicație, orice obiect virtual, un computer sau un serviciu.

## Trusted Platform Module

Un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). De obicei un Trusted Platform Module este instalat pe placa de bază a computerului și interacționează cu alte componente ale sistemului prin magistrala hardware.

## Informații despre codurile de la terți

Informațiile despre codurile de la terți sunt conținute în fișierul legal\_notices.txt din directorul de instalare al aplicației.

## Note privind mărcile comerciale

Mărcile înregistrate și mărcile de servicii sunt în proprietatea deținătorului lor de drept.

Adobe, Acrobat și Shockwave sunt mărci comerciale sau mărci comerciale înregistrate ale Adobe Systems Incorporated în Statele Unite ale Americii și/sau în alte țări.

Mac și FireWire sunt mărci comerciale ale Apple Inc. înregistrate în Statele Unite ale Americii și în alte țări.

AutoCAD este o marcă comercială sau o marcă comercială înregistrată a Autodesk, Inc. și/sau a afiliaților săi în Statele Unite ale Americii și în alte țări.

Bluetooth și sigla corespunzătoare sunt proprietatea Bluetooth SIG, Inc.

Borland este o marcă comercială sau o marcă comercială înregistrată a Borland Software Corporation în Statele Unite ale Americii și în alte țări.

Citrix și Citrix Provisioning Services sunt mărci comerciale ale Citrix Systems, Inc. și/sau a filialelor sale înregistrate la biroul de brevetare din Statele Unite ale Americii și din alte țări.

dBase este o marcă comercială a dataBased Intelligence, Inc.

EMC și SecurID sunt mărci comerciale sau mărci comerciale înregistrate ale EMC Corporation în SUA și în alte țări.

ICQ este o marcă comercială și/sau marcă de serviciu a ICQ LLC.

Intel și Pentium sunt mărci comerciale ale Intel Corporation înregistrate în Statele Unite ale Americii și în alte țări.

Logitech este o marcă comercială sau o marcă comercială înregistrată a Logitech Company în SUA și în alte țări.

Mail.ru este o marcă comercială înregistrată a Mail.Ru, LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell și Surface sunt mărci comerciale ale Microsoft Corporation, înregistrate în Statele Unite ale Americii și în alte țări.

Mozilla și Thunderbird sunt mărci comerciale ale Mozilla Foundation.

Novell este o marcă comercială a Novell Inc., înregistrată în Statele Unite ale Americii și în alte țări.

Java și JavaScript sunt mărci comerciale înregistrate ale Oracle Corporation și/sau ale afiliaților săi.

SafeNet este marca comercială înregistrată a SafeNet, Inc.

UNIX este o marcă comercială înregistrată în Statele Unite ale Americii și în alte țări și este utilizată sub licență de la X/Open Company Limited.